Universidad Carlos III de Madrid
Escuela Politécnica Superior
Grado en Ingeniería Telemática

Análisis de la conectividad de usuarios en una red de campus 802.11

Trabajo Fin de Grado

Autor: Mario Rodríguez Blanco
Tutor: Pablo Serrano Yáñez-Mingot
Director: Carlos Jesús Bernardos Cano

Marzo de 2015

Agradecimientos

En primer lugar dar las gracias a mis padres, por darme la oportunidad de estudiar una carrera y por demostrarme su apoyo y alegría según iba superando asignaturas.

Agradecer también a todos mis compañeros de universidad que me han acompañado durante estos años. A Carlos y a Sergio por acompañarme durante la gran mayoría de este camino. Y en especial a Alberto, José Manuel y Pablo por haber formado parte de este grupo desde el primer día hasta el último, sin los cuales este camino habría sido mucho más duro.

Resumen

A lo largo de estos últimos años, el desarrollo de las redes de telecomunicaciones ha sufrido un fuerte crecimiento. Dichas redes disponen de una gran variedad de técnicas de acceso. Una de las técnicas de más éxito es mediante comunicación inalámbrica. Debido a que nos hemos convertido en una sociedad cada vez más móvil, la demanda de redes inalámbricas por parte de los usuarios está incrementando exponencialmente, gracias a la movilidad que permiten.

Otros de los motivos de dicho incremento son la facilidad de instalación y mantenimiento, los costes relativamente bajos en comparación con las redes cableadas o la popularización de los dispositivos móviles (smartphones, tablets, ordenadores portátiles).

Estas ventajas han conllevado a que el tráfico de datos (WiFi y banda ancha móvil) de las redes inalámbricas sea cada vez mayor, llegando a superar el 50% del tráfico total de Internet en 2012, siendo los usuarios conectados a WiFi los que generan la mayor parte del tráfico de datos inalámbricos. Se espera que el tráfico de banda ancha fija sea cada vez menor.

Puesto que la evolución de las redes inalámbricas es constante y que cada vez su existencia es mayor, requiere las habilidades de supervisión, de análisis y de resolución de problemas específicas para WiFi. Hace unos años el principal objetivo de estas redes era la cobertura de la señal. Hoy en día se necesita buena calidad, interferencias bajas y un buen uso del canal de distribución. Además, la necesidad de la seguridad dentro de una red inalámbrica es esencial. Poder detectar y bloquear ataques antes de que infecten la red es imprescindible.

Otra de las motivaciones para analizar las redes inalámbricas es la preocupación de los usuarios en cuanto a la privacidad de la localización. Esta preocupación se debe a que las aplicaciones basadas en la localización, que utilizan GPS y otras tecnologías de posicionamiento, podrían revelar esta información sin desearlo. Sin embargo la privacidad de la ubicación se ve amenazada incluso por dispositivos que no la rastrean explícitamente.

Las redes inalámbricas cada vez están más presentes en lugares públicos como pueden ser centros comerciales, bibliotecas, estaciones, aeropuertos, universidades, etc. El principal problema de estas redes es que la información que se transmite es susceptible de ser capturada por cualquier usuario, ya que los datos viajan por el aire.

Este hecho permite realizar diversos análisis: identificar usuarios, detectar caídas de equipos, analizar la cobertura, velocidad y uso de la red, etc.

A pesar de la herencia compartida, WiFi (802.11) no es Ethernet. Tiene un número adicional de características, cada una de las cuales pueden causar problemas. Conocer estos problemas a veces requiere un administrador de la red para llegar a los detalles de nivel bajo. Los sistemas de análisis de red están reconocidos como una herramienta útil en las redes cableadas; en las redes inalámbricas son seguramente más importantes, ya que en una red 802.11 pueden ocurrir más problemas.

Existen cinco áreas fundamentales a la hora de llevar un modelo de gestión de red útil: gestión de rendimiento, gestión de fallos, gestión de configuración, gestión de cuentas y gestión de seguridad.

Los datos anteriores sobre redes inalámbricas y la necesidad de supervisar su funcionamiento mediante una monitorización y su posterior análisis, han sido los principales motivos para la realización del Trabajo Fin de Grado.

Este Trabajo Fin de Grado consiste en el análisis de la conectividad de usuarios en una red de campus 802.11 mediante herramientas de captura y análisis de tráfico. El objetivo es diseñar e implementar un programa que realice escaneos periódicos de la red y almacenar la información en una base de datos, para su posterior análisis.

Para la consecución de dicho objetivo se llevarán a cabo las siguientes tareas: estudio del funcionamiento de una aplicación de análisis de redes y descripción de una red 802.11, desarrollo de un programa basado en la tarea anterior, creación de una base de datos para almacenar la información, realización de pruebas y correcciones hasta llegar al funcionamiento esperado y analizar la información almacenada.

La primera fase consiste en el estudio de alguna herramienta o aplicación que permita averiguar qué dispositivos están conectados a la red, para conocer su funcionamiento. La mayoría de los dispositivos modernos están conectados a través de una red común. En casa tenemos smartphones, tablets, ordenadores, consolas e incluso electrodomésticos conectados entre sí. En la oficina seguramente tenemos equipos de sobremesa, servidores o impresoras configurados de manera que puedan comunicarse y compartir datos.

A la hora de realizar el estudio del funcionamiento de una aplicación de análisis de redes, hemos elegido la aplicación *Fing*, que permite conocer todos los equipos conectados a la red, ofreciendo información sobre la misma y los dispositivos conectados a ésta. Todos los dispositivos se identifican con su dirección IP, dirección MAC, nombre y fabricante.

Para conocer el funcionamiento de la aplicación, necesitamos capturar el intercambio de mensajes que se realiza mientras se está ejecutando el escaneo de la red, utilizando la herramienta de captura Wireshark.

Se realizará una explicación sobre el intercambio de mensajes del protocolo ARP, describiendo su cabecera y sus campos, y se mostrará un diagrama de señalización de dicho intercambio, para comprender mejor su funcionamiento.

Para conocer el nombre de cada dispositivo, *Fing* realiza peticiones DNS (*Domain Name System*) a cada dirección IP que pertenece a la red, aunque no todos los dispositivos tienen asignado un nombre.

En paralelo a este estudio se realizará una descripción de una red LAN (*Local Area Network*) inalámbrica, WLAN o WiFi. Hay muchas diferencias entre un dispositivo 802.11 y un dispositivo Ethernet, pero la más obvia es que los dispositivos 802.11 son móviles, lo que permite desplazarse de una parte de la red a otra.

Se describirán las principales características de una red 802.11, así como los componentes que la forman: sistema de distribución, puntos de acceso, medio inalámbrico y estaciones. Se analizarán los tipos de redes existentes y los servicios de red que ofrece.

En relación a esta descripción, se describirán las opciones disponibles en el campus para conectarse a una red inalámbrica. La Universidad Carlos III ofrece dos posibilidades para conectarse a su red inalámbrica (*WiFi-UC3M* y *eduroam*). Los usuarios podrán optar entre una de las dos, según sus necesidades y las posibilidades del terminal.

En la segunda fase se diseñará e implementará el programa en consecuencia al estudio previo de la aplicación.

Para ello se definirá la estructura que tendrá el sistema a desarrollar, que estará compuesto por cinco partes fundamentales:

- Pc del laboratorio
- Programa
- Base de datos MySQL
- Consultas
- Análisis de resultados

Como hemos visto en el análisis, necesitamos disponer de un cliente ARP para detectar los usuarios que se conectan a la red. Para ello utilizaremos como base el cliente ARP diseñado en la asignatura Redes y Servicios de Comunicaciones Avanzadas. Dependiendo del tamaño de la red, realizar las peticiones a todas las direcciones IP que puedan estar conectadas puede tardar demasiado tiempo para llevar un seguimiento adecuado. Por este motivo se realizaron dos tipos de clientes ARP en función de la manera en que se realizan las peticiones.

En el primer cliente ARP, las peticiones se realizarán en secuencia, es decir, una a una. Esto se debe a que se quiere testear el buen funcionamiento del programa en la red del laboratorio, puesto que la red es pequeña. El funcionamiento de este cliente ARP es sencillo. Se mandan peticiones a cada dirección de la red en secuencia hasta que se preguntan por todas las posibles, cuando se vuelve a repetir el proceso.

Una vez que comprobamos que los resultados son los mismos que si lanzamos la aplicación *Fing* a la vez, vemos que el funcionamiento es correcto. Por lo tanto cada vez que obtenemos un nuevo usuario, almacenamos su información en la base de datos. El siguiente paso es probar el funcionamiento en una red más grande y escaneando en el interfaz inalámbrico. De las dos redes inalámbricas disponibles (*WiFi-UC3M* y *eduroam*) comenzamos probando el programa en *eduroam*.

El funcionamiento del programa en *eduroam* es correcto, pero al cabo de las ejecuciones no permite realizar más peticiones. Esto es debido a la seguridad que posee *eduroam*, que al advertir demasiadas peticiones broadcast ARP, deniega la posibilidad de continuar mandando peticiones, para evitar posibles ataques de inundación en la red. Por lo tanto la red inalámbrica elegida para realizar los escaneos y posteriores análisis será *WiFi-UC3M*.

En *WiFi-UC3M* el programa sigue funcionando según lo esperado, monitorizando la red durante un mes. El problema de esta red es que es mayor que *eduroam*. Esto implica que para realizar un escaneo completo de la red realizando las peticiones en secuencia se emplea demasiado tiempo, aproximadamente 50 min de media, dependiendo del número de usuarios conectados. Con tanto tiempo entre cada escaneo no se pueden obtener datos concluyentes.

En el segundo cliente ARP se realizarán las peticiones en paralelo, es decir, mediante ráfagas. Esto se debe a que se quiere testear el buen funcionamiento del programa en *WiFi-UC3M*, una red grande que requiere un tiempo de escaneo menor.

Para disminuir el tiempo de duración del escaneo, tanto el envío como la recepción de peticiones se realizan mediante hilos. Para ello el hilo de envío manda

peticiones en ráfagas de X direcciones cada X ms, mientras que el hilo de recepción se queda a la espera de recibir tramas.

El objetivo es realizar escaneos cada 5 o 10 minutos para realizar un buen seguimiento de los usuarios. Para llevar un seguimiento constante se realizará un escaneo completo de la red cada 10 min, aunque el tiempo total de escaneo sea algo menor.

Con esta configuración y con el correspondiente almacenamiento de los datos obtenidos en la base de datos, el funcionamiento del programa es el previsto, monitorizando la red durante un período amplio de tiempo como para hacer un estudio sobre la red.

Para almacenar los datos obtenidos del programa se han creado las siguientes tablas:

En la tabla “Direcciones”, se almacena la información sobre cada usuario encontrado en la red, guardando su dirección IP, dirección MAC, RTT (*Round-Trip delay Time*) de la petición, número de ejecución asociado a cada escaneo y fecha y hora en la que se ha realizado la petición.

En la tabla “Ejecuciones”, se almacena el tiempo en que se realiza cada escaneo, guardando el identificador único de cada entrada y la fecha y hora en la que se ha realizado el escaneo.

En la tabla “Marcas”, se almacena los rangos de direcciones MAC son su correspondiente marca.

Finalmente se realizarán distintos análisis sobre los datos recogidos. Para ello se creará un programa que, mediante consultas a la información almacenada en la base de datos, obtenga los resultados para mostrarlos.

Abstract

Over recent years, the development of telecommunication networks has suffered a strong growth. Such networks have a variety of access techniques in which the success of wireless communication has to be highlighted. Due to the fact of having become an increasingly mobile society; the demand of wireless networks by users is growing exponentially due to the mobility they allow.

Other reasons of that increase are the ease of installation and maintenance, the relatively low cost it has compared to wired networks or the popularization of mobile devices (smartphones, tablets, laptops).

These advantages have improved data traffic (WiFi and mobile broadband) wireless networks, exceeding 50% of total Internet traffic in 2012, where users connected to WiFi have been the ones generating more traffic. Besides, fixed broadband is expected to decrease.

Since the evolution of wireless networks is constant and its existence is greater, skills of supervision, analysis and resolution of specific problems of WiFi are required. A few years ago the main objective of these networks was the signal coverage. Nowadays a decent quality, low interference and good use of the distribution channel are needed. Furthermore, the need of security in a wireless network is essential. Being able to detect and block attacks before inflecting the network is essential.

Another motivation for analyzing wireless networks is the concern of users regarding the privacy of location. This fear is because applications based on location using GPS and other positioning technologies could unwittingly disclose this information. However, location privacy is threatened even for devices that do not explicitly track.

Wireless networks are increasingly present in public places such as shopping malls, libraries, stations, airports, universities, etc. The main problem of these networks is that the information transmitted is likely to be captured by any user because data moves through the air.

This allows different analysis: identify users, equipment outages detect, analyze coverage, speed and network usage, etc.

Despite the shared heritage, WiFi (802.11) is not Ethernet. It has a number of additional features, each of which can cause problems. Knowing these problems

requires sometimes a network administrator to reach the low-level details. The network analysis systems are recognized as a useful tool in wired networks; although they are probably more important in wireless networks because within an 802.11 network more problems may occur.

There are five essential areas of carrying a model useful network management: performance management, fault management, configuration management, account management and security management.

The above data about wireless networks and the need to supervise their performance through monitoring and subsequent analysis were the main reasons for implementing the Bachelor Thesis.

This Bachelor Thesis consists on the analysis of the connectivity of users in an 802.11 campus network by capturing tools and traffic analysis. The objective is to design and implement a program performing periodic scans of the network and storing the information in a database for later analysis.

To achieve this objective the following, these tasks will be performed: study of the operation of an application of network analysis and description of an 802.11 network; developing a task based on the previous program; creation of a database to store the information; testing and corrections to reach the expected performance and analyze the stored information.

The first phase involves the study of any tool or application that can find out which devices are connected to the network, in order to understand its functioning. Most modern devices are connected through a common network. At home we have smartphones, tablets, computers, consoles and even domestic appliances connected. In the office we probably have desktops, servers or printers configured so that they can communicate and share data.

To realize the study of an application of network analysis, we selected the Fing application, which identifies all connected devices to the network providing information of itself and also about the ones connected to this equipment. All devices are identified by their IP address, MAC address, name and manufacturer.

To know the operation of the application, we need to capture the message exchange performed while running the network scan, using the Wireshark capture.

Fing performs requests ARP (Address Resolution Protocol) to find out which IP addresses have been assigned within the network. We will know that an address has no being assigned if after the timeout it has been no response. With this mechanism Fing

can find out all the devices connected to the network, knowing your IP address and MAC address.

To understand how the ARP protocol is working, an explanation of the message exchange is performed, describing his head and fields, and a signaling diagram of the exchange will be displayed.

Fing performs DNS (Domain Name System) requests to each IP address belonging to the network to know the name of each device although not all devices are assigned a name.

A description of a LAN (Local Area Network) wireless network (WLAN or WiFi) will be made. There are many differences between an 802.11 device and an Ethernet device, but the most obvious one is that 802.11 devices are mobile, allowing you to move from one part of the network to another.

The main characteristics of a network 802.11 will be described, as well as the components comprising it: distribution system, access points, wireless medium and stations. The types of networks and network services offered will be discussed.

In relation to this description, the options available in the campus to connect to a wireless network will be explained. University Carlos III of Madrid offers two ways of connecting to your wireless network (WiFi-UC3M and eduroam). Users may choose between one of them, depending on their needs and possibilities of the terminal.

In the second phase the program will be designed and implemented accordingly to the previous study of the application.

The structure of the system will consist of five main parts:

- PC
- Program
- MySQL Database
- Consultations
- Analysis of results

As we have seen in the analysis, a ARP client is needed to detect users who connect to the network. We will use the ARP client base designed in the course Networks and Services Advanced Communications. Depending on the size of the network, make requests to all IP addresses that can be connected may take too long to be monitored closely. Therefore, two types of ARP client will be designed depending on the way the requests are asked to be realized.

In the first ARP client, requests will be made in sequence, i.e. one by one. This is because we want to test the proper functioning of the program in the lab network, since the network is small. This operation of this ARP client is simple Requests sequentially to each network address are sent, until it asks for all, when the process is repeated.

Once we see that the results are the same as if we launched the Fing application at a time, we see that it is functioning properly. So whenever we get a new user, we store his information in the database. The next step is to test the performance in a larger network and scann on the wireless interface. From the two available wireless networks (WiFi-UC3M and eduroam), we begin testing the program in eduroam.

The operation of the program in eduroam is correct, but after executions it does not allow more requests. This is because of the security eduroam has, noticing that too many broadcast ARP have been requested, it denied the possibility to continue sending requests to avoid possible flooding attacks on the network. Thus the wireless network chosen for scans and further analysis will be WiFi-UC3M.

In WiFi-UC3M the program still works as expected, scanning the network for a month. The problem of this network is that it is larger than eduroam. This implies that for a full scan of the network by performing sequential requests too many time is spent, about 50 min on average, depending on the number of connected users. With so much time between each scan no conclusive data can be obtained.

In the second ARP client, requests will be made on parallel, ie by bursts. This is because we want to test the proper functioning of the program in WiFi-UC3M, a large network requiring a shorter scan. To reduce the duration of the scan, both sending and receiving requests are made by threads. For this, the thread shipping sends requests in bursts of X addresses every X ms, while the reception thread waits to receive frames.

The goal is to perform scans every 5 or 10 minutes to do a good tracking users. To keep a constant monitoring, we will perform a complete network scan every 10 minutes, although the total scan time is somewhat smaller.

With this configuration and the corresponding storage of data in the database, the operation of the program is planned, scanning the network for an extended period of time to do a study on the network.

To store the data of the program, we have created the following tables:

In the "Addresses" table, information about each user found in the network is stored, keeping his IP address, MAC address, RTT (Round-Trip Time delay) of the petition, execution number associated with each scan, and date and time which the request was made.

In the "Executions" table, we store the time in which each scan has been done, keeping the unique identifier for each entry and the date and time when the scan was performed.

In the "Brands" table, MAC address ranges are stored corresponding brand.

Finally, different analysis of the data collected will be made. For this, we will design a program which, by querying the information stored in the database, gets the results to display them.

Índice general

Índice de figuras

Índice de tablas

CAPÍTULO I

INTRODUCCIÓN

I. INTRODUCCIÓN

En este capítulo se describen los principales aspectos y su consecuente motivación por la que se ha optado a realizar este Trabajo Fin de Grado, junto con los objetivos que persigue y la estructura del documento.

1.1. Descripción y motivación

Hasta el día de hoy, todas las entidades públicas y privadas disponen de redes de telecomunicaciones fijas que se deben a unas decisiones de implantación de soluciones que en su momento cumplían las necesidades de los usuarios en servicios como el teléfono, la televisión, internet, etc. Estas decisiones suponían unas inversiones elevadas.

Las redes de telecomunicaciones actuales disponen de una gran variedad de técnicas de acceso. Una de las técnicas de más éxito es mediante una comunicación inalámbrica. Esta técnica permite aprovechar las ventajas de la propagación de las ondas vía radio para ofrecer al usuario el acceso a la red sin cables de red y, por tanto, mayor movilidad. La comunicación inalámbrica ha evolucionado hasta el punto de ser capaz de ofrecer conectividad a Internet a un gran número de usuarios en áreas extensas. Las redes inalámbricas ofrecen varias ventajas sobre las redes fijas o cableadas [1]:

Movilidad

Los usuarios se mueven, pero los datos normalmente se almacenan de forma centralizada. Permitir a los usuarios acceder a los datos mientras están en movimiento puede llevar a grandes aumentos de la productividad.

Facilidad y rapidez de despliegue

En muchas áreas es difícil desplegar la infraestructura necesaria para una red cableada tradicional. Los edificios más antiguos a menudo son un problema; instalar el cableado a través de las paredes de un edificio de piedra antiguo en el que los planos se han perdido puede ser un desafío. En muchos lugares históricos, las leyes de conservación hacen que sea difícil llevar a cabo las nuevas instalaciones de redes. Incluso en edificios modernos la contratación de la instalación del cableado conlleva un gran coste y consume mucho tiempo.

Flexibilidad

Inalámbrico significa que no hay cableado. Esto permite a los usuarios crear redes "amorfas" rápidamente y en cualquier lugar. La expansión de las redes inalámbricas es fácil porque el medio de red está disponible en todas partes. La flexibilidad es el gran punto de venta para el mercado de "punto caliente", compuesto por hoteles, aeropuertos, estaciones, bibliotecas y cafeterías.

Coste

En algunos casos, los costes se pueden reducir mediante el uso de la tecnología inalámbrica. Por ejemplo, la infraestructura 802.11, más conocida como WiFi, puede ser utilizada para crear un puente inalámbrico entre dos edificios. La creación de un puente inalámbrico requiere cierto coste de capital inicial en términos de equipos exteriores, puntos de acceso e interfaces inalámbricas. Después del desembolso inicial, mantener una red basada en 802.11 sólo tendrá un coste operativo mensual recurrente insignificante.

Estas ventajas han conllevado a que el tráfico de las redes inalámbricas sea cada vez mayor. En 2012 el tráfico de datos inalámbricos (Wifi y banda ancha móvil) superó el 50% del tráfico de Internet global. Se espera que en los próximos años el tráfico de banda ancha fija sea cada vez menor. En 2017, más del 60% del tráfico mundial de Internet procederá de conexiones WiFi. En la Figura 1 se pueden apreciar la previsión de tráfico de datos (%) hasta 2017 [2].

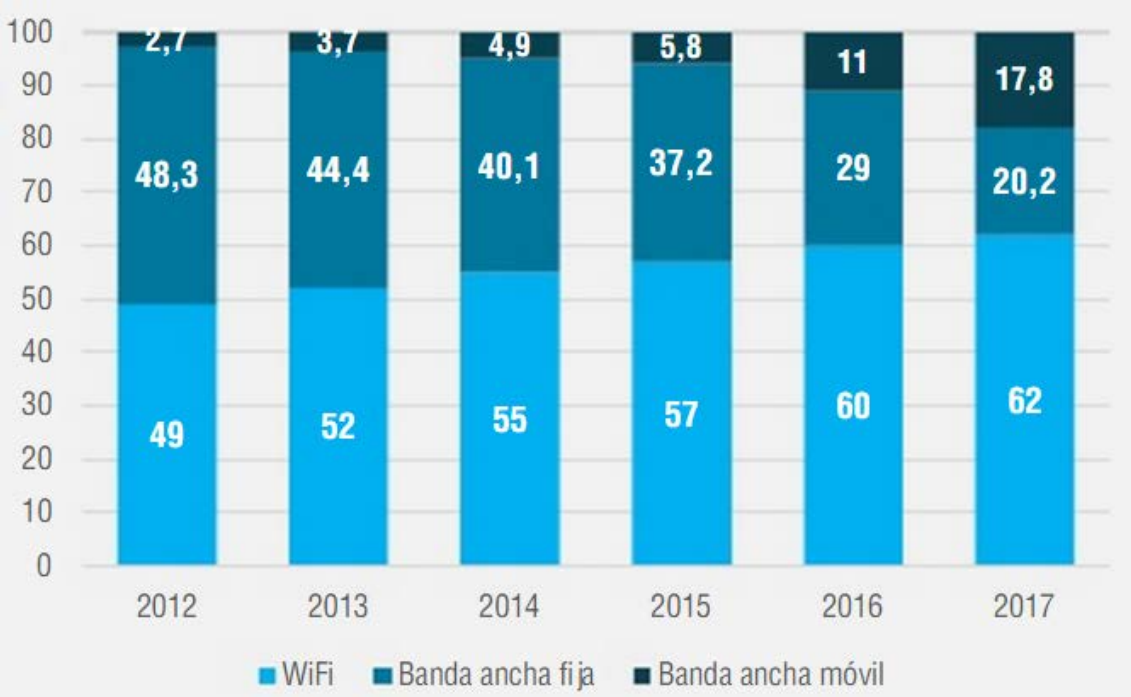


Figura 1. Previsión de tráfico de datos

En cuanto a usuarios conectados a WiFi, se superó el 30% respecto del total de la población con acceso a Internet [2]. En la Figura 2 podemos ver la previsión de la población conectada a WiFi, que se espera que se acerque al 60% de la población total en 2017.

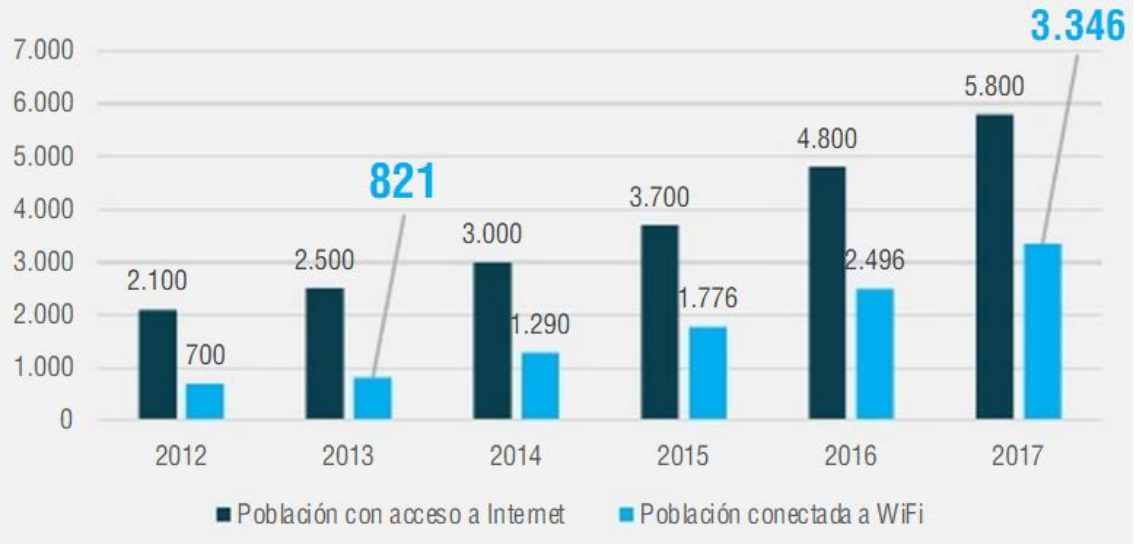


Figura 2. Previsión de población con acceso a Internet vs conectada a WiFi

El tráfico mundial de datos móviles creció un 69% en 2014, una tasa comparable a la de 2012, pero menor que el crecimiento de 2013, que fue un año "rebote" tras la desaceleración de 2012. El creciente número de dispositivos inalámbricos que tienen acceso a las redes móviles en todo el mundo es uno de los principales contribuyentes al crecimiento mundial del tráfico móvil. En la Figura 3 se puede apreciar la previsión de la cantidad de dispositivos móviles en los próximos 5 años. Entre paréntesis se pueden ver los porcentajes correspondientes al año 2014 [3].

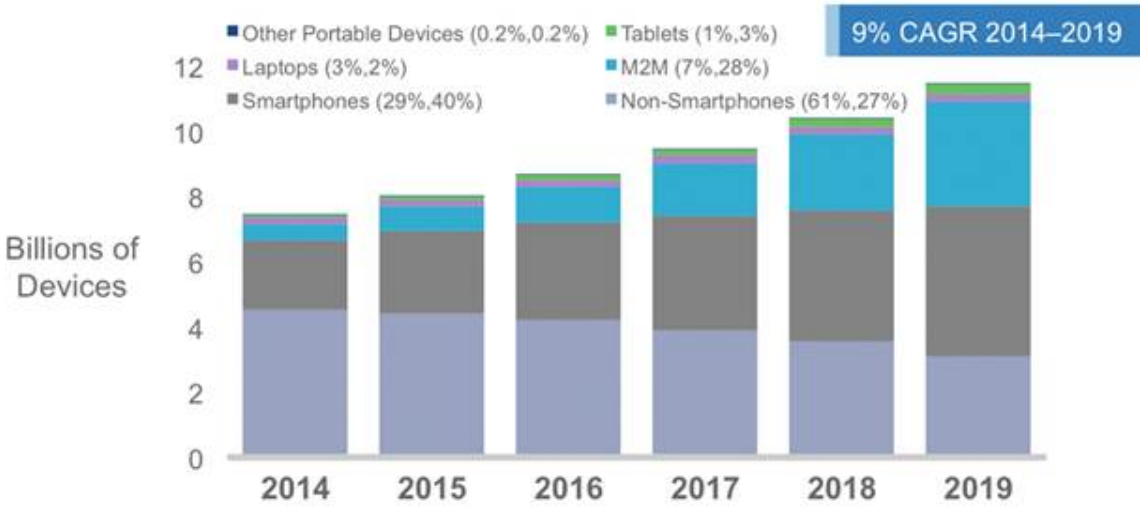


Figura 3. Previsión de dispositivos móviles

El incremento de los dispositivos inalámbricos repercutirá considerablemente en el tráfico móvil. Se espera que el tráfico global de datos móviles crezca hasta 24,3 exabytes por mes en 2019, casi un aumento de diez veces en comparación con 2014. El tráfico de datos móviles crecerá a una tasa compuesta anual del 57% desde 2014 hasta 2019, como se puede apreciar en la Figura 4 [3].

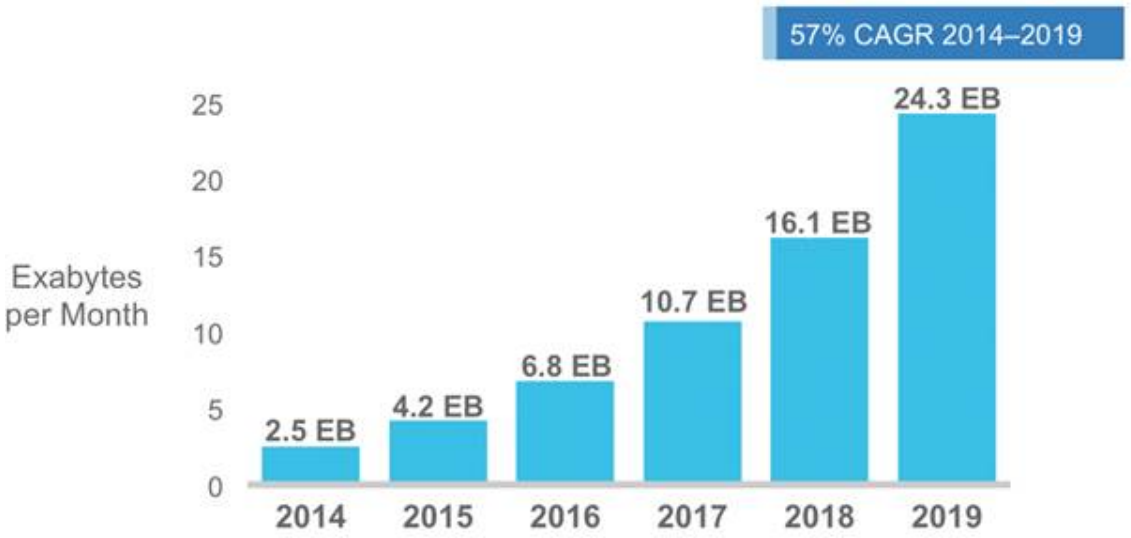


Figura 4. Previsión de tráfico de datos móviles

Puesto que la evolución de las redes inalámbricas es constante y que cada vez su existencia es mayor, requiere las habilidades de supervisión, de análisis y de resolución de problemas específicas para WiFi. Hace unos años el principal objetivo de estas redes era la cobertura de la señal, proporcionar un servicio aceptable en un área bien cubierta. Hoy en día para admitir voz, vídeo y aplicaciones de alto rendimiento se necesita buena calidad, interferencias bajas y un buen uso del canal de distribución. Además, la necesidad de la seguridad dentro de una red inalámbrica es esencial. Poder detectar y bloquear ataques antes de que infecten la red es imprescindible.

A pesar de la herencia compartida, 802.11 no es Ethernet. Tiene un número adicional de características, cada una de las cuales pueden causar problemas. Conocer estos problemas a veces requiere un administrador de la red para llegar a los detalles de nivel bajo. Los sistemas de análisis de red están reconocidos como una herramienta útil en las redes cableadas; en las redes inalámbricas son seguramente más importantes, ya que en una red 802.11 pueden ocurrir más problemas.

La Organización Internacional para la Estandarización (ISO) ha creado un modelo de gestión de red útil, definiendo cinco áreas [4]:

Gestión de rendimiento

El objetivo es cuantificar, medir, informar, analizar y controlar el rendimiento de los distintos componentes de red. Estos componentes son los dispositivos individuales (enlaces, routers, host), así como las abstracciones entre extremos, tales como un camino a través de la red. Algunos protocolos sencillos de gestión de red como SNMP (*Simple Network Management Protocol*) juegan un importante papel en la gestión del rendimiento de Internet.

Gestión de fallos

El objetivo es registrar, detectar y responder a las condiciones de fallo en la red. La gestión de fallos se puede ver como el control inmediato de los fallos transitorios de la red, mientras que la gestión de rendimiento proporciona, a largo plazo, niveles aceptables de rendimiento respecto a demandas diversas de tráfico y fallos ocasionales en los dispositivos de red. El protocolo SNMP también juega un papel central en la gestión de fallos.

Gestión de configuración

Permite al administrador de red hacer un seguimiento de los dispositivos de red y de las configuraciones hardware y software de estos dispositivos.

Gestión de cuentas

Permite al administrador de red especificar, registrar y controlar el acceso de los usuarios y dispositivos a los recursos de la red. Tanto las cuotas de uso, como facturación basada en el uso, o como la asignación de privilegios de acceso a recursos, corresponden a la gestión de cuentas.

Gestión de seguridad

El objetivo es controlar el acceso a los recursos de red de acuerdo a alguna política bien definida. Los centros de distribución de claves y las autoridades de certificación, son componentes de la gestión de seguridad. Otro componente crucial son los cortafuegos, que supervisan y controlan los puntos externos de acceso a la red.

Otra de las motivaciones para analizar las redes inalámbricas es la preocupación de los usuarios en cuanto a la privacidad de la localización [5]. Esta preocupación se debe a que las aplicaciones basadas en la localización, que utilizan GPS y otras tecnologías de posicionamiento, podrían revelar esta información sin desearlo. Sin embargo la privacidad de la ubicación se ve amenazada incluso por dispositivos que no

la rastrean explícitamente. Típicamente los usuarios WiFi se conectan a puntos de acceso cercanos, por lo que conociendo la ubicación del punto de acceso se puede obtener una ubicación aproximada del usuario. Además los sistemas de monitorización pueden utilizar la intensidad de la señal inalámbrica para precisar con más detalle su ubicación.

La identificación de los usuarios individuales es a menudo trivial, ya que los dispositivos WiFi utilizan nombrados de forma única por sus direcciones MAC. En algunos sistemas, como la red de teléfono GSM o Bluetooth, utilizan seudónimos para ocultar la identidad del usuario. Este es un primer paso necesario para hacer más difícil el seguimiento de estas redes. Otro mecanismo ha sido usado recientemente en los dispositivos con iOS 8, que a la hora de buscar redes inalámbricas generan una dirección MAC aleatoria. De esta forma ningún punto de acceso podrá saber con seguridad si el dispositivo que manda la petición es el mismo que mandó una similar anteriormente [6].

Teniendo en cuenta los datos anteriores sobre redes inalámbricas, en concreto sobre WiFi, y la necesidad de supervisar su funcionamiento mediante una monitorización y su posterior análisis, se ha optado por realizar un estudio sobre la conectividad de los usuarios en una red 802.11.

1.2. Objetivos

El principal objetivo de este Trabajo Fin de Grado consiste en el diseño e implementación de un programa que realice escaneos periódicos de la red de la universidad para posteriormente analizar la conectividad de sus usuarios. Para la consecución de dicho objetivo se van a realizar las siguientes tareas:

- Estudio del funcionamiento de una aplicación de análisis de redes.
- Desarrollo de un programa basado en el punto anterior.
- Creación de una base de datos para almacenar la información.
- Realización de pruebas y correcciones hasta llegar al funcionamiento esperado.
- Analizar la información almacenada.

1.3. Estructura de la memoria

En esta sección se hace una breve presentación del contenido del documento, con la finalidad de facilitar su lectura. El documento consta de 8 capítulos:

Capítulo I. Introducción: en este capítulo se realiza una introducción general de la descripción y motivación del Trabajo Fin de Grado, junto con los objetivos que persigue.

Capítulo II. Introduction: en este capítulo se realiza una introducción general de la descripción y motivación del Trabajo Fin de Grado, junto con los objetivos que persigue, pero en lengua inglesa.

Capítulo III. Estado del arte: en este capítulo se realiza una descripción de los protocolos 802.11 y ARP, y de las redes inalámbricas disponibles en el campus de la Universidad Carlos III de Madrid. También se hace un estudio sobre una aplicación de análisis de redes.

Capítulo IV. Diseño: en este capítulo se realiza una descripción del diseño del programa a desarrollar.

Capítulo V. Análisis resultados: en este capítulo se analizan los resultados obtenidos mediante gráficos.

Capítulo VI. Conclusiones y trabajos futuros: en este capítulo se exponen las reflexiones y resoluciones obtenidas tras la realización de este Trabajo Fin de Grado

Capítulo VII. Conclusions and future works: en este capítulo se exponen las reflexiones y resoluciones obtenidas tras la realización de este Trabajo Fin de Grado, pero en lengua inglesa.

Capítulo VIII. Anexos: en este capítulo se detalla la planificación, el marco regulador y el presupuesto del proyecto.

CAPÍTULO II

INTRODUCTION

II. INTRODUCTION

This chapter describes the main aspects on completing the Bachelor Thesis.

2.1. Description and motivation

Until today, all public and private entities have fixed telecommunications networks to be some decisions implementing solutions that once met the needs of users in services such as telephone, television, internet, etc. These decisions assumed high investments.

Current telecommunications networks offer a variety of access techniques. One of the most successful techniques is by wireless communication. This technique takes advantage of the propagation of radio waves to give users access to the network without network cables and, therefore, greater mobility. Wireless communication has evolved to the point of being able to offer Internet connectivity to a large number of users over large areas. Wireless networks offer several advantages over fixed networks or wired [1]:

Mobility

Users move, but data is usually stored centrally. Enabling users to access data while they are in motion can lead to large productivity gains.

Ease and speed of deployment

Many areas are difficult to wire for traditional wired LANs. Older buildings are often a problem; running cable through the walls of an older stone building to which the blueprints have been lost can be a challenge. In many places, historic preservation laws make it difficult to carry out new LAN installations in older buildings. Even in modern facilities, contracting for cable installation can be expensive and time-consuming.

Flexibility

No cables means no recabling. Wireless networks allow users to quickly form amorphous, small group networks for a meeting, and wireless networking makes moving between cubicles and offices a snap. Expansion with wireless networks is easy because the network medium is already everywhere. There are no cables to pull,

connect, or trip over. Flexibility is the big selling point for the "hot spot" market, composed mainly of hotels, airports, train stations, libraries, and cafes.

Cost

In some cases, costs can be reduced by using wireless technology. As an example, 802.11-equipment can be used to create a wireless bridge between two buildings. Setting up a wireless bridge requires some initial capital cost in terms of outdoor equipment, access points, and wireless interfaces. After the initial capital expenditure, however, an 802.11-based, line-of-sight network will have only a negligible recurring monthly operating cost. Over time, point-to-point wireless links are far cheaper than leasing capacity from the telephone company.

These advantages have led to traffic in wireless networks is growing. In 2012 wireless data traffic (Wifi and mobile broadband) exceeded 50% of global Internet traffic. It is expected that in the coming years the fixed broadband traffic is diminishing. In 2017, over 60% of global Internet traffic will come from WiFi connections. In Figure 1 can be seen the data traffic forecast (%) 2017 [2].

Figure 1. Forecast data traffic

As users connected to WiFi, exceeded 30% of the total population with access to Internet [2]. In Figure 2 we can see the forecast of the population connected to WiFi, which is expected to approach 60% of the total population in 2017.

Figure 2. Forecast of population with access to Internet vs connected to WiFi

Global mobile data traffic grew 69% in 2014, a rate comparable to that of 2012 but lower than the growth in 2013, which was a year "rebound" after the slowdown in 2012. The increasing number of wireless devices that access to mobile networks around the world is one of the major contributors to global growth of mobile traffic. Figure 3 shows the forecast of the number of mobile devices in the next five years. Between brackets you can see the percentages for the year 2014 [3].

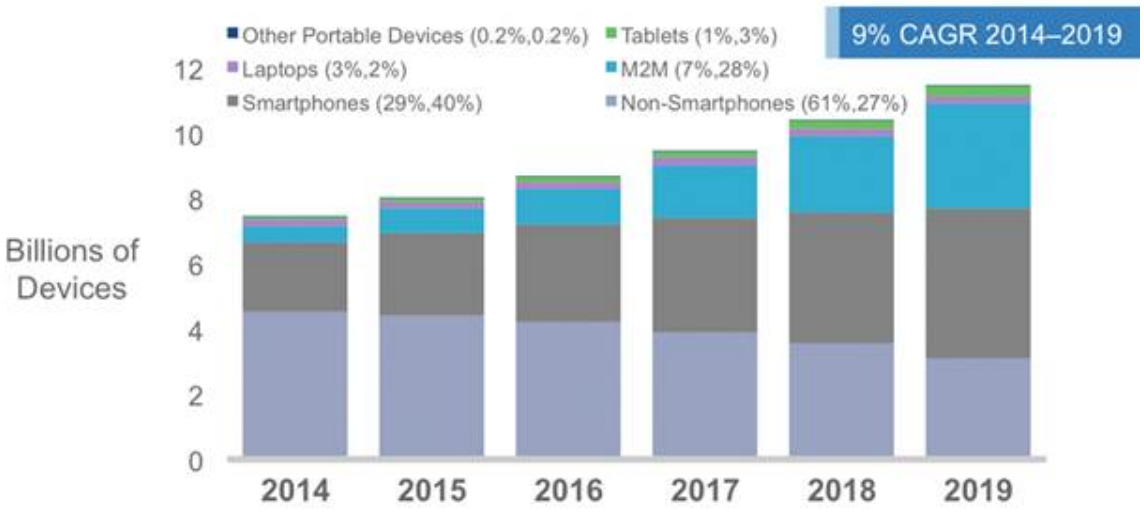


Figure 3. Forecast of mobile devices

The increase of wireless devices has a significant impact on the mobile traffic. Expected global mobile data traffic to grow to 24.3 exabytes per month in 2019, almost a tenfold increase compared to 2014. Mobile data traffic will grow at a CAGR of 57% from 2014-2019, as can be seen in Figure 4 [3].

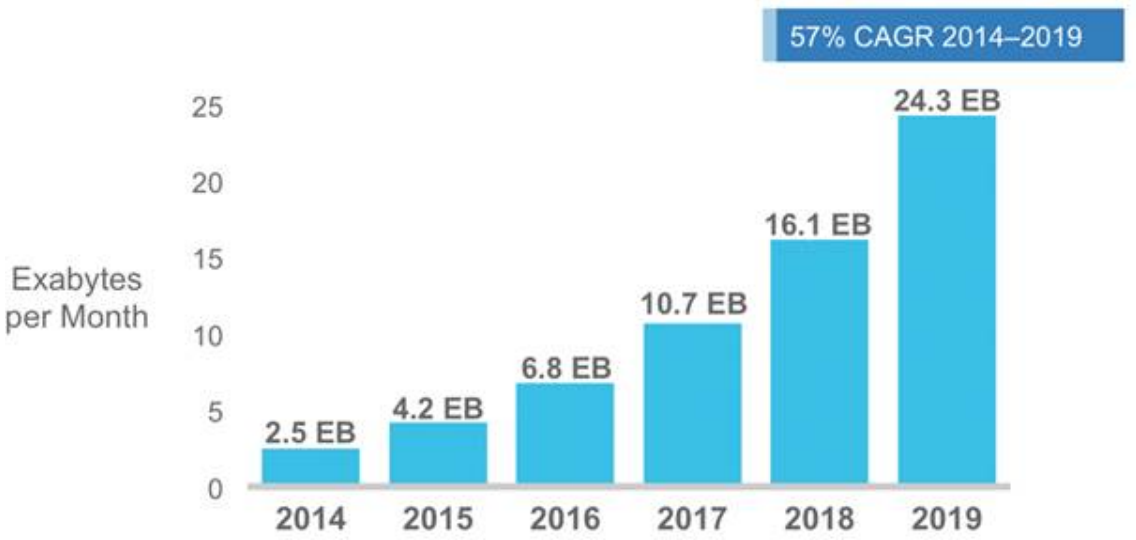


Figure 4. Forecast of mobile data traffic

In spite of the shared heritage, 802.11 is not Ethernet. It has a number of additional protocol features, each of which can cause problems. Fixing problems on 802.11 networks sometimes requires that a network administrator get down to the low-level protocol details and see what is happening over the airwaves. Network analyzers have long been viewed as a useful component of the network administrator's toolkit on wired networks for their ability to report on the low-level details. Analyzers on wireless networks will be just as useful, and possibly even more important. More things can go wrong on an 802.11 network, so a good analyzer is a vital tool for quickly focusing troubleshooting on the likely culprit.

The International Organization for Standardization (ISO) has developed a model useful network management, defining five areas [4]:

Performance Management

The objective is to quantify, measure, report, analyze and monitor the performance of different network components. These components are individual devices (links, routers, host) and between ends abstractions, such as a path through the network. Some simple network management protocols such as SNMP (*Simple Network Management Protocol*) play an important role in the management of Internet performance.

Fault Management

The aim is to record, detect and respond to fault conditions in the network. Fault management can be seen as the immediate control of transient network failures, while

providing performance management, long term, acceptable levels of performance over various traffic demands and occasional failures in network devices. The SNMP protocol also plays a central role in fault management.

Configuration Management

Allows the network administrator to monitor network devices and the hardware configurations and software of these devices.

Account Management

Allows the network administrator to specify record and control user access and devices to network resources. Both user fees, such as usage-based billing, or assigning access privileges to resources correspond to account management.

Security management

The objective is to control access to network resources according to some well-defined policy. Distribution centers and key certification authorities are components of security management. Another crucial component is the firewall, which monitor and control external access points to the network.

Another motivation for analyzing wireless networks is the concern of users regarding the privacy of the location [5]. This concern is that location-aware applications, which use GPS and other positioning technologies, might reveal this information in undesirable ways. However, location privacy is threatened even by devices that do not explicitly track location. Since 802.11 users usually associate with access points that are less than tens of meters away, knowing the access point that a user is associated with gives away a coarse estimate of his location. Moreover, systems that can employ multiple monitoring locations can use wireless signal strength to obtain an even more accurate estimate of a user's location.

Identifying individual users is often trivial since the 802.11 devices that they use are uniquely named by their MAC addresses. In some systems, such as GSM telephone network or Bluetooth, used pseudonyms to conceal the identity of the user. This is necessary to make it harder to track these networks. Another mechanism was recently used on devices with iOS 8, when searching for wireless networks generate a random MAC address. Thus any access point can know for sure if the device that sends the request is the same as sent a similar previously [6].

Given the above data over wireless networks, specifically on WiFi, and the need to monitor their performance through monitoring and further analysis, it was decided to conduct a study on the connectivity of users in an 802.11 network.

2.2. Objectives

The main objective of this Bachelor Thesis involves the design and implementation of a program to perform periodic scans of the network of college and then analyze the connectivity of its users. To achieve this objective are to perform the following tasks:

- Study the operation of an application of network analysis.
- Development of a point based on the previous program.
- Creating a database for storing information.
- Testing and corrections to reach the expected performance.
- Analyze the stored information.

CAPÍTULO III

ESTADO DEL ARTE

III. ESTADO DEL ARTE

En este capítulo se realiza una descripción del protocolo 802.11, de las redes inalámbricas disponibles en el campus de la Universidad Carlos III de Madrid y del protocolo ARP. También se hace un estudio sobre una aplicación de análisis de redes.

3.1. 802.11

Una LAN (*Local Area Network*) inalámbrica, WLAN o WiFi, es un sistema de transmisión de datos para proporcionar acceso a la red independientemente de la ubicación entre los dispositivos, por medio de ondas de radio en lugar de una infraestructura de cable. 802.11 es superficialmente similar a Ethernet. Entender el fondo de Ethernet ayuda ligeramente a comprender el funcionamiento de 802.11, pero hay una gran cantidad de tecnología adicional para adaptar el Ethernet tradicional a un ámbito inalámbrico. Hay muchas diferencias entre un dispositivo 802.11 y un dispositivo Ethernet, pero la más obvia es que los dispositivos 802.11 son móviles, lo que permite fácilmente desplazarse de una parte de la red a otra.

3.1.1. Características

802.11 es un miembro de la familia IEEE 802 (*Institute of Electrical and Electronics Engineers*) y es una serie de especificaciones para las tecnologías de red de área local, LAN. Las especificaciones IEEE 802 se centran en las dos capas más bajas del modelo OSI (*Open System Interconnection*) (Figura 5), porque incorporan componentes tanto de la capa física, como de la capa de enlace de datos.

Figura 5. Modelo OSI

La subcapa MAC (*Media Acces Control*) se encarga de determinar la forma de acceder al medio y enviar datos, mientras que la capa física (PHY) se encarga de los detalles de la transmisión y la recepción de datos. Como se puede ver en la Figura 6, todas las redes 802 tienen un componente tanto de la subcapa MAC como de la capa PHY.

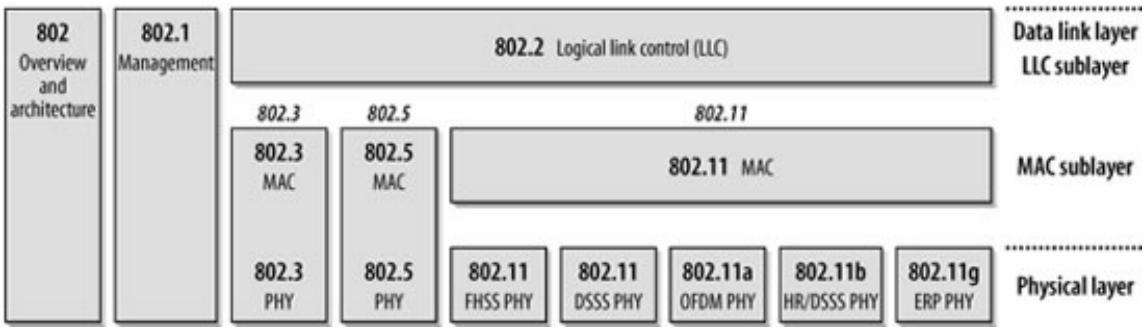


Figura 6. Familia 802 y modelo OSI

Las especificaciones individuales de la familia 802 se identifican con un segundo número. En la Tabla 1 se pueden ver los distintos estándares [7].

Estándares	Descripción	Estado
802.1	Higher Layer LAN Protocols	Activo
802.2	Logical Link Control	Disuelto
802.3	Ethernet	Activo
802.4	Token Bus	Disuelto
802.5	Token Ring	Disuelto
802.6	Metropolitan Area Network	Disuelto
802.7	Broadband TAG	Disuelto
802.8	Fiber Optic TAG	Disuelto
802.9	Integrated Services LAN	Disuelto
802.10	Security	Disuelto
802.11	Wireless Local Area Network (WLAN)	Activo
802.12	Demand Priority	Disuelto
802.13		-
802.14	Cable Modem	Disuelto
802.15	Wireless Personal Area Network (WPAN)	Activo
802.16	Broadband Wireless Access	Activo
802.17	Resilient Packet Ring	Hibernando
802.18	Radio Regulatory	Activo
802.19	Wireless Coexistence	Activo
802.20	Mobile Broadband Wireless Access (MBWA)	Hibernando
802.21	Media Independent Handover Services	Activo
802.22	Wireless Regional Area Networks	Activo
802.23	Emergency Services	Disuelto
802.24	Smart Grid	Activo

Tabla 1. Estándares familia 802

3.1.2. Componentes

Las redes 802.11 están compuestas por cuatro grandes componentes físicos [1]:

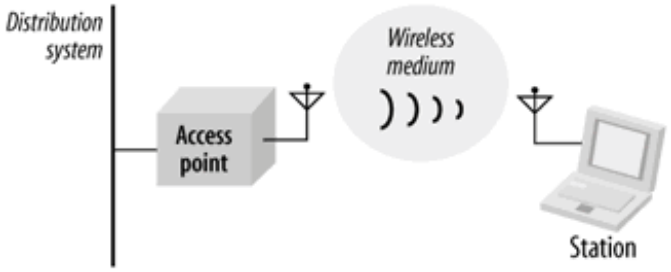


Figura 7. Componentes redes 802.11

- **Sistema de distribución:** encargado de enviar las tramas a su destino.
- **Punto de acceso (AP):** funciona de puente entre el medio inalámbrico y el cableado.
- **Medio inalámbrico:** popularmente formado por capas físicas de radiofrecuencia.
- **Estaciones:** dispositivos con interfaces de red inalámbricas.

3.1.3. Tipos de redes

El bloque básico de una red 802.11 es el BSS (*Basic Service Set*), y es un grupo de estaciones que se comunican entre sí. Las comunicaciones tienen lugar dentro de un área llamada área de servicio básico, definida por las características de propagación del medio inalámbrico. Cuando una estación se encuentra en el área de servicio básico, puede comunicarse con los otros miembros del BSS. Existen dos tipos de BSS [1]:

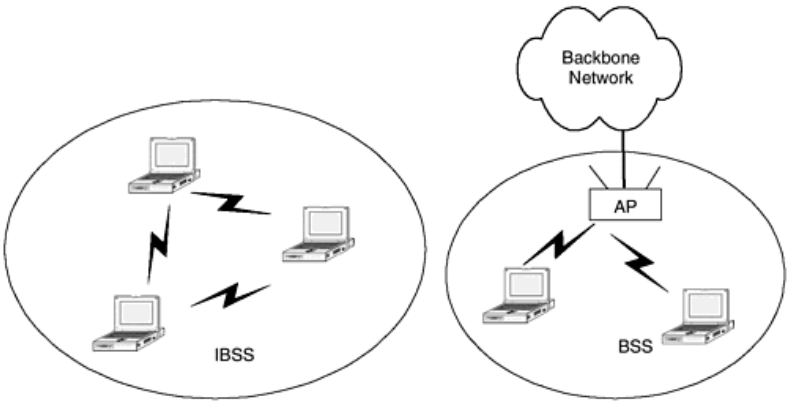


Figura 8. BSSs independiente e infraestructura

Redes independientes (IBSS o modo ad-hoc)

Las estaciones en una IBSS (*Independent Basic Service Set*) se comunican directamente entre sí. La red 802.11 más pequeña posible es una IBSS con dos

estaciones. Debido a su corta duración, pequeño tamaño y propósito, también son llamadas BSS ad-hoc o redes ad-hoc.

Redes de infraestructura

Las redes de infraestructura se distinguen por el uso de un AP. Los APs se utilizan para todas las comunicaciones. La principal ventaja de estas redes, es que las estaciones móviles no necesitan estar cerca para mantener una comunicación, ya que con estar dentro del área de servicio básico del AP es suficiente. Para unirse a esta red, las estaciones deben asociarse con el AP, proceso equivalente a conectar el cable de red en una red Ethernet. Las estaciones siempre inician el proceso de asociación, y el AP concede o deniega el acceso según el contenido de la solicitud. Una estación móvil puede estar asociada a un único AP.

Áreas de servicio extendido

802.11 permite crear redes inalámbricas de gran tamaño vinculando varios BSSs, formando una red ESS (*Extended Service Set*). Las estaciones móviles pueden comunicarse entre sí a pesar de que puedan estar en diferentes áreas de servicio básico. Para ello el medio inalámbrico tiene que actuar como una sola conexión de la capa de enlace. En el escenario de la Figura 9, el router utiliza una única dirección MAC para entregar las tramas a una estación móvil, la dirección del AP al que está asociada la estación móvil. El router no conoce la ubicación de dicha estación, únicamente entrega las tramas al AP.

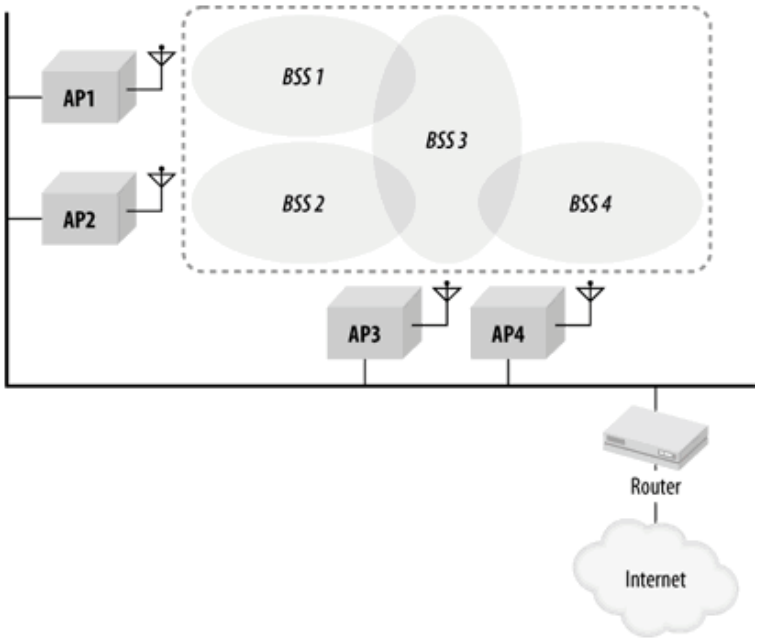


Figura 9. Escenario ESS

3.1.4. Servicios de red

Una forma de definir una tecnología de red es definir los servicios que ofrece y de qué forma permite a los proveedores de equipos implementarlos según consideren conveniente. 802.11 proporciona nueve servicios [1]; tres de ellos se utilizan para comunicar los datos, el resto son operaciones de gestión que permiten a la red realizar un seguimiento de los nodo móviles para transmitir las tramas de forma correcta.

- **Distribución:** servicio utilizado en la entrega de tramas para determinar la dirección de destino en las redes de infraestructura.
- **Integración:** entrega de tramas a una red no inalámbrica.
- **Asociación:** se utiliza para establecer el punto de acceso que sirve de puerta de enlace para la estación móvil.
- **Reasociación:** se utiliza para cambiar el punto de acceso que sirve de puerta de enlace para la estación móvil.
- **Disociación:** elimina la estación móvil de la red.
- **Autenticación:** establece la identidad antes de permitir la asociación.
- **Deautenticación:** termina la autenticación y por tanto la asociación.
- **Privacidad:** proporciona protección ante posibles ataques.
- **Entrega MSDU:** entrega los datos al receptor.

3.2. 802.11 en el campus

La red WiFi de la UC3M [8] es un medio de acceso complementario a la red de cable. Su uso está indicado cuando las necesidades de ancho de banda no son muy exigentes. Para acceder a una red WiFi es imprescindible disponer de una tarjeta o interfaz WiFi compatible con la norma 802.11 a/b/g/n. También es necesario tener activado en dicho interfaz el protocolo de configuración automática DHCP (*Dynamic Host Configuration Protocol*) y eliminar cualquier servidor proxy en el navegador.

En la actualidad la cobertura WiFi es estimada en un valor alrededor del 90%. En los departamentos de Ingeniería Telemática y de Teoría de la Señal del edificio Torres Quevedo han elegido instalar su propia red WiFi. La Universidad Carlos III ofrece dos posibilidades para conectarse a su red inalámbrica. Los usuarios podrán optar entre una de las dos, según sus necesidades y las posibilidades del terminal.

3.2.1. *WiFi-UC3M*

Es una red abierta que no precisa de ningún tipo de credenciales (login y password) y que permite la navegación web y el uso de lectores de correo basados en IMAP (*Internet Message Access Protocol*) seguro, sin necesidad de ninguna

configuración. Este servicio, sin embargo, exige la aceptación al comienzo de cada sesión de las condiciones de uso establecidas por el Vicerrectorado de Calidad, Infraestructuras y Medio Ambiente. Dicho mensaje se puede ver en la Figura 10.

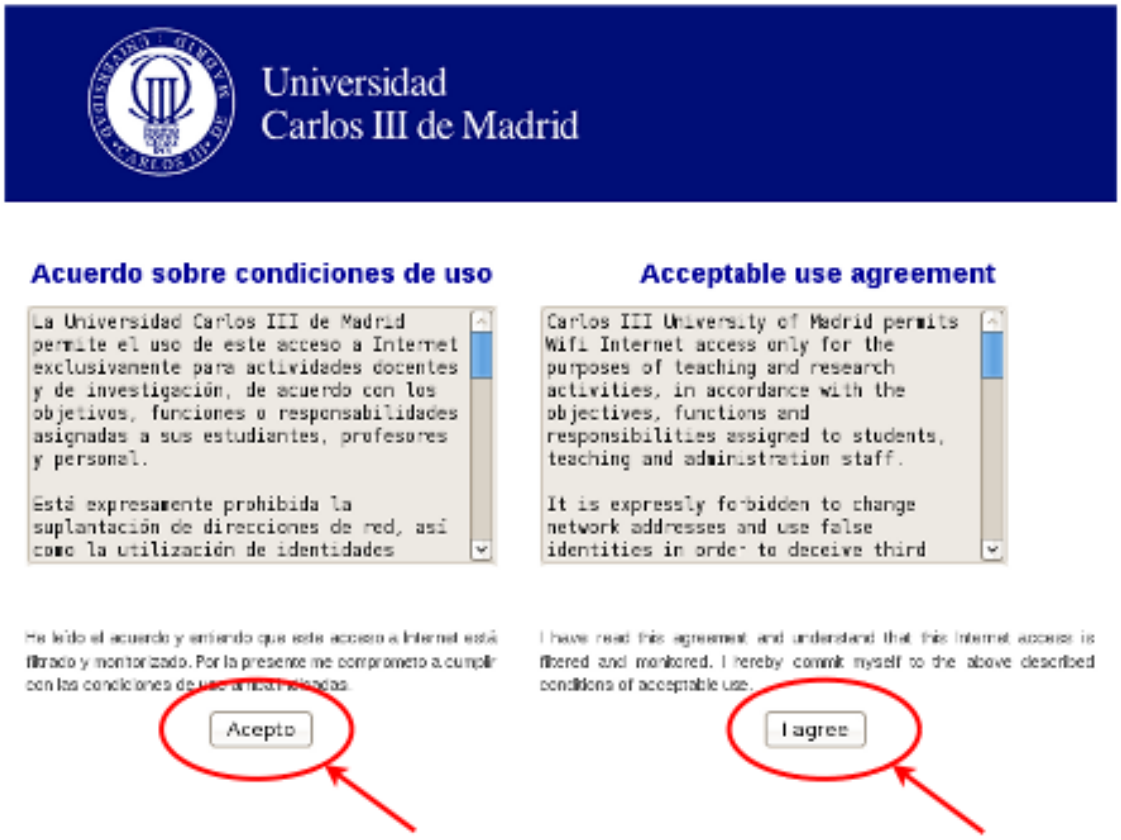


Figura 10. Condiciones de uso *WiFi-UC3M*

El texto informativo con dichas condiciones se presentará al abrir su navegador y sólo tras su aceptación se podrá hacer uso de la red (Figura 11).

Como contrapartida a su facilidad de uso, debe tenerse presente que esta red constituye un medio inseguro, ya que no protege las comunicaciones contra posibles escuchas por parte de otros usuarios. Otro inconveniente es que no permite el acceso a recursos electrónicos a los que se accede a través de determinados proxies [8].

Figura 11. Mensaje autenticación *WiFi-UC3M*

3.2.2. *Eduroam*

Esta red permite un acceso completo a los servicios de datos o aplicaciones de la Universidad o de Internet en general, excepto a aquellos que están restringidos por condiciones particulares. Los servicios accesibles son, por tanto, idénticos a los disponibles desde cualquier PC de despacho o aula informática. Las aplicaciones P2P (*Peer to Peer*) de descarga de contenido son filtradas por esta red y por tanto no deben utilizarse. Esta red proporciona al usuario un buen nivel de seguridad, ya que el tráfico se cifra usando claves de sesión generadas de forma automática (estándar 802.1X).

Eduroam es una red autenticada, para utilizarla es necesario disponer de una Cuenta de Servicios de Red, la misma que se usa para acceder al correo electrónico de la UC3M. También se permite el acceso a todo aquel que disponga de una cuenta similar en alguna de las instituciones adscritas al proyecto *MovIRIS/EDUROAM*. Así mismo, los usuarios de la UC3M podrán usar su cuenta habitual para conectarse a la red *eduroam* de cualquiera de las instituciones asociadas [8].

Para poder utilizar la red, tanto la tarjeta inalámbrica (802.11 a/b/g/n) como el sistema operativo, deben soportar WPA. Para que la presente configuración funcione correctamente es necesario que la contraseña esté almacenada en un determinado formato. Por este motivo se debe comprobar que la contraseña es correcta en la Guía de

configuración de *eduroam* [9]. Los datos mínimos para la configuración de la red son los siguientes:

- **SSID:** *eduroam*
- **Autenticación de red:** 802.1X (PEAP)
- **Cifrado:** WPA2/AES (recomendado) o WPA/TKIP

En el caso de que no se haya conseguido realizar la configuración, se dispone del instalador EDUROAM CAT (*Configuration Assistant Tool*) para su descarga y ejecución. También ofrece la alternativa de utilizar las siguientes guías para configuración paso a paso en distintos sistemas operativos [9]:

Figura 12. Sistemas operativos disponibles *eduroam*

3.3. ARP

El protocolo ARP [10] pertenece a la capa de enlace de datos y es el responsable de averiguar la dirección MAC que corresponde a una determinada dirección IP.

Cuando ARP necesita resolver una dirección MAC dada la dirección IP, envía un paquete *arp request* a la dirección de difusión de la red (broadcast) FF:FF:FF:FF:FF:FF que contiene la dirección MAC e IP de origen y la dirección IP de destino. Cada host en la red local recibe este mensaje y el host con la dirección IP de destino envía un paquete *arp reply* al host origen con su dirección MAC y su dirección IP. La cabecera de un mensaje ARP es la siguiente:

Tipo de hardware	2 bytes
Tipo de protocolo	2 bytes
Longitud dirección de hardware en bytes (x) / Longitud dirección de protocolo en bytes (y)	2 bytes
Código de operación	2 bytes
Dirección hardware del emisor	x bytes
Dirección IP del emisor	y bytes
Dirección hardware del receptor	x bytes
Dirección IP del receptor	y bytes

Figura 13. Cabecera ARP

El contenido de los campos de la cabecera para el envío de un *arp request* es el siguiente:

- **Tipo de hardware:** 0x0001 (Ethernet)
- **Tipo de protocolo:** 0x0800 (IP)
- **Longitud dirección de hardware:** 6
- **Longitud dirección de protocolo:** 4
- **Código de operación:** 0x0001 (*arp request*)
- **Dirección hardware del emisor:** dirección MAC origen
- **Dirección IP del emisor:** dirección IP origen
- **Dirección hardware del receptor:** 00:00:00:00:00:00
- **Dirección IP del receptor:** dirección IP destino

El diagrama de señalización en una petición ARP se muestra en la siguiente figura, donde el host con dirección IP 192.168.1.4 desea saber la dirección MAC del host con dirección IP 192.168.1.3:

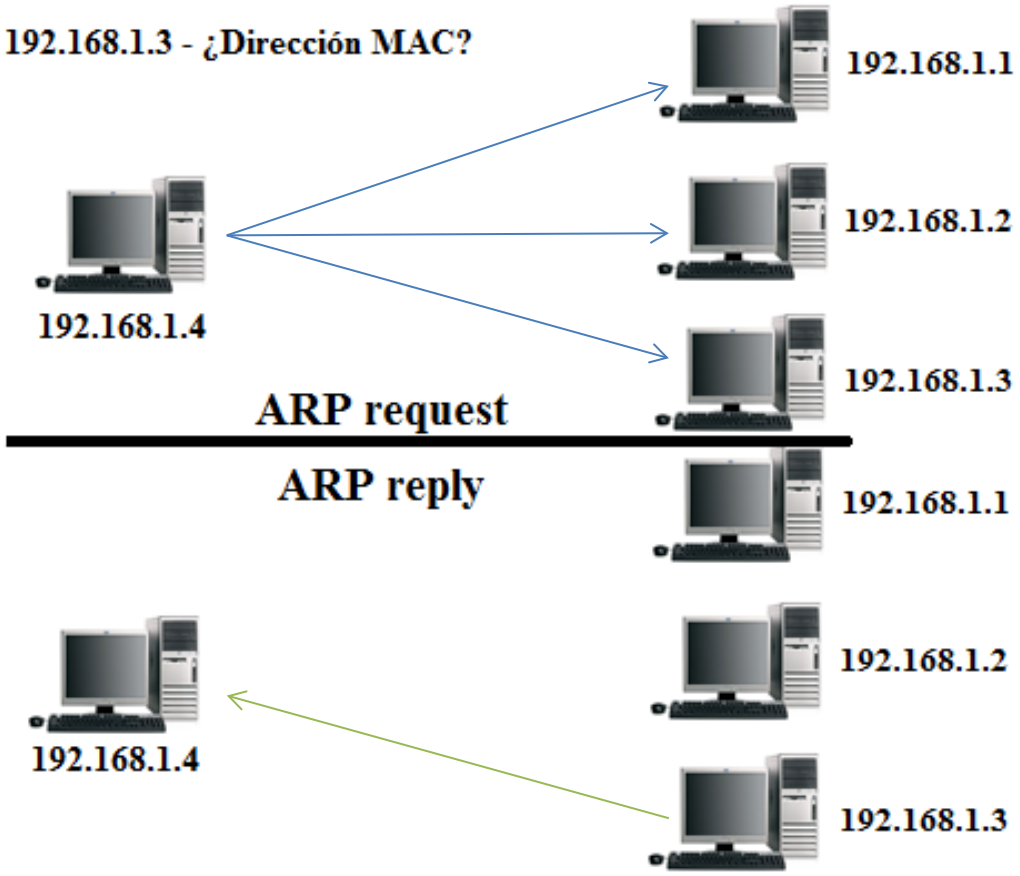


Figura 14. Diagrama de señalización ARP

3.4. *Fing*

Para llevar a cabo el estudio del funcionamiento de una aplicación de análisis de redes hemos elegido la aplicación *Fing*.

La mayoría de los dispositivos modernos están conectados a través de una red común. En casa tenemos smartphones, tablets, ordenadores, consolas e incluso electrodomésticos conectados entre sí. En la oficina seguramente tenemos equipos de sobremesa, servidores o impresoras configurados de manera que puedan comunicarse y compartir datos [11].

Figura 15. *Fing*: Logo

3.4.1. Características

Fing es una herramienta multiplataforma gratuita [12] [13] que permite conocer de forma rápida todos los equipos conectados a la red, ofreciendo gran cantidad de información sobre la misma y sobre los dispositivos conectados a ésta. Es una aplicación profesional para el análisis de redes con una interfaz simple e intuitiva que ayuda a evaluar los niveles de seguridad, detectar intrusos y resolver problemas de red.

Fing detecta automáticamente el tipo de red y utiliza la técnica más adecuada para encontrar los dispositivos conectados. Todos los dispositivos se identifican con direcciones de red, nombre y fabricante. Los mejores resultados se obtienen en redes Ethernet y WiFi, donde *Fing* puede beneficiarse de un motor de descubrimiento con una gran nitidez y velocidad. Los resultados se pueden compartir a través de correo electrónico y en muchos formatos estándar, para una fácil integración con otras aplicaciones.

Una vez detectados los dispositivos en la red, se puede realizar un análisis más profundo con los servicios que presta a través de los puertos. *Fing* es capaz de reconocer distintos servicios, incluyendo los más comunes como servicio Web (HTTP, *Hypertext*

Transfer Protocol), servicio de transferencia de archivos (FTP, *File Transfer Protocol*) y servicio de nombres de dominio (DNS) [11].

3.4.2. Uso

Al acceder a la aplicación comienza a escanear la red a la que estamos conectados. A partir de la dirección IP de la red y de la máscara de subred calcula el número máximo de hosts que pueden estar conectados. Una vez hecho esto comienza a enviar peticiones a todas las direcciones IP calculadas en el paso anterior y almacena todas las respuestas. Por lo tanto cuanto más grande sea la red, más tiempo tardará en realizar el escaneo completo.

Como se puede ver en la Figura 16, en la parte superior tenemos el nombre de la red y el número de hosts activos al realizar la última búsqueda. A continuación se muestra una lista con los hosts conocidos hasta el momento y la siguiente información:

- **Icono:** indica si se trata de un router, host, smartphone, impresora, etc.
- **Dirección IP:** dirección IP del dispositivo, resaltando los octetos destinados a la dirección del host.
- **Dirección MAC:** dirección MAC del dispositivo. Se puede especificar que no se muestre por completo por motivos de privacidad.
- **Nombre:** nombre de la máquina.
- **Fabricante:** fabricante de la tarjeta de red del dispositivo.

Al presionar sobre el nombre de la red, podemos ver algunas de sus características y diversas opciones (Figura 16), como cambiar el orden en que se muestran los dispositivos o compartir dicha red.

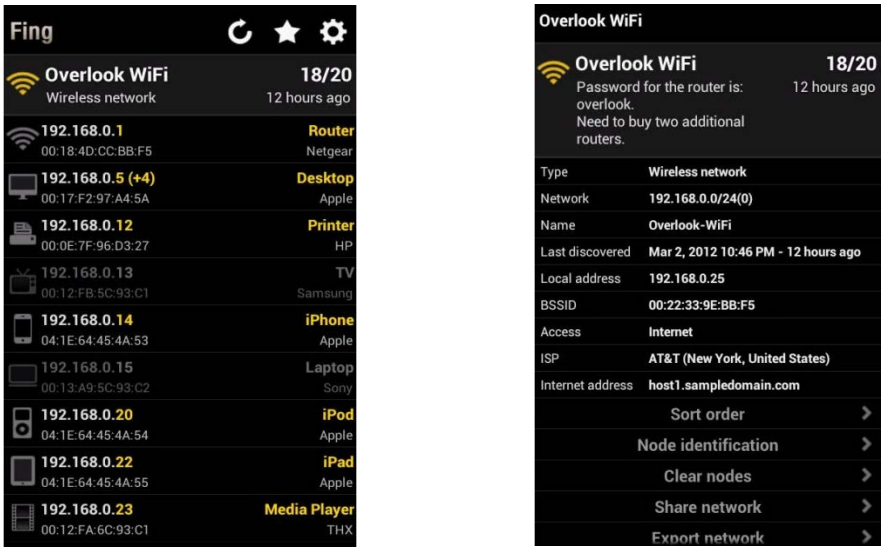


Figura 16. *Fing*: Menú y características red

Los dispositivos que aparecen en un tono grisáceo son aquellos cuya presencia ya detectó la aplicación en un análisis anterior, pero cuando se realizó el último análisis no estaban conectados.

Al presionar sobre cualquier dispositivo de la lista se puede acceder a distintas opciones (Figura 17). A parte de editar el nombre y añadir una descripción, nos permite hacer varias cosas interesantes, como por ejemplo escanear los puertos del equipo y averiguar qué servicios ofrece, hacer un ping (Figura 18), trazar la ruta desde nuestro dispositivo hasta él, o incluso enviar una petición Wake on LAN para arrancarlo (Figura 19), siempre y cuando el equipo permita este tipo de arranque.

En la opción de escanear los puertos para averiguar qué servicios ofrece, se puede seleccionar cualquiera de ellos y *Fing* ejecutará la aplicación encargada de conectarnos utilizando el protocolo seleccionado. En caso de no disponer de alguna aplicación que ofrezca dicho servicio, se mostrará la aplicación conveniente en la tienda de aplicaciones para poder descargarla.

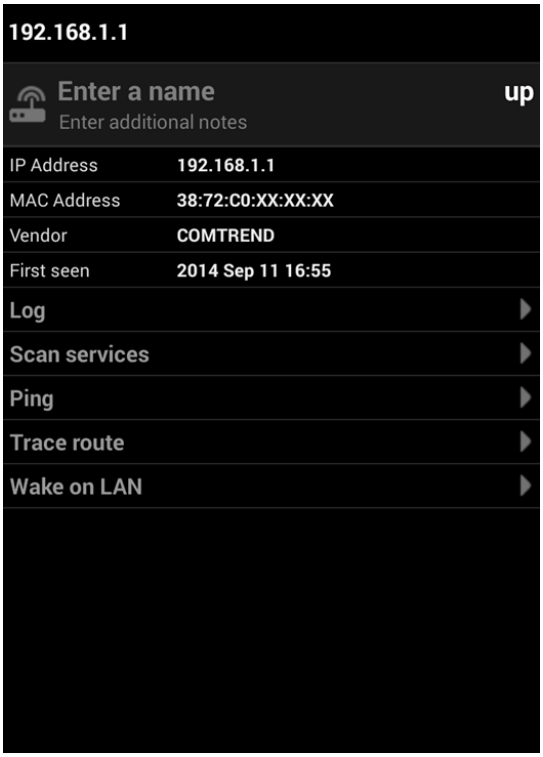


Figura 17. *Fing*: Opciones dispositivo

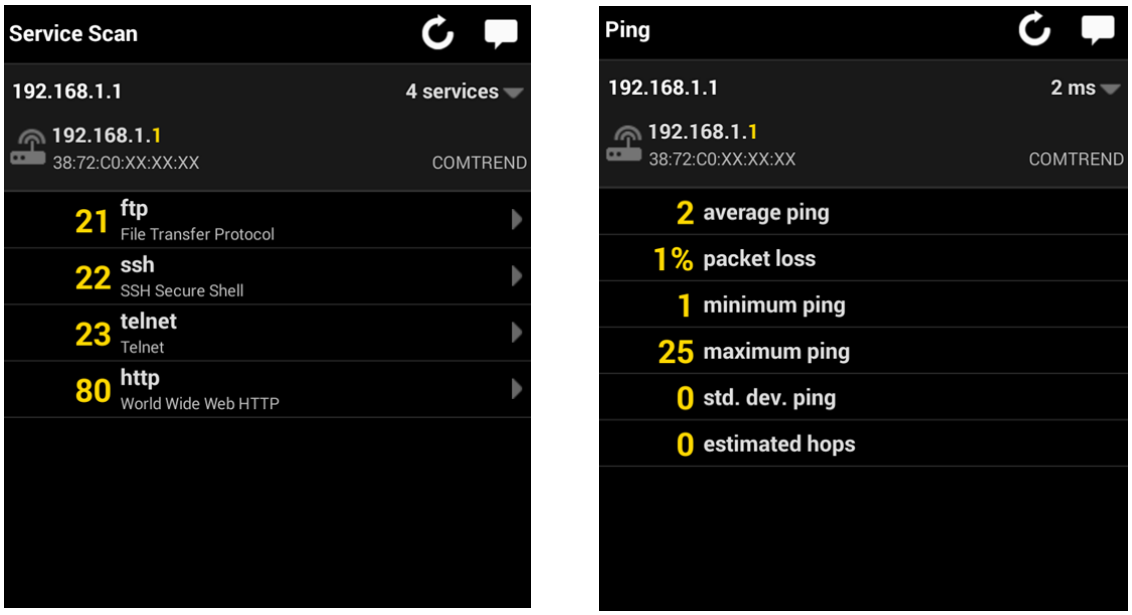


Figura 18. *Fing*: Service Scan y Ping

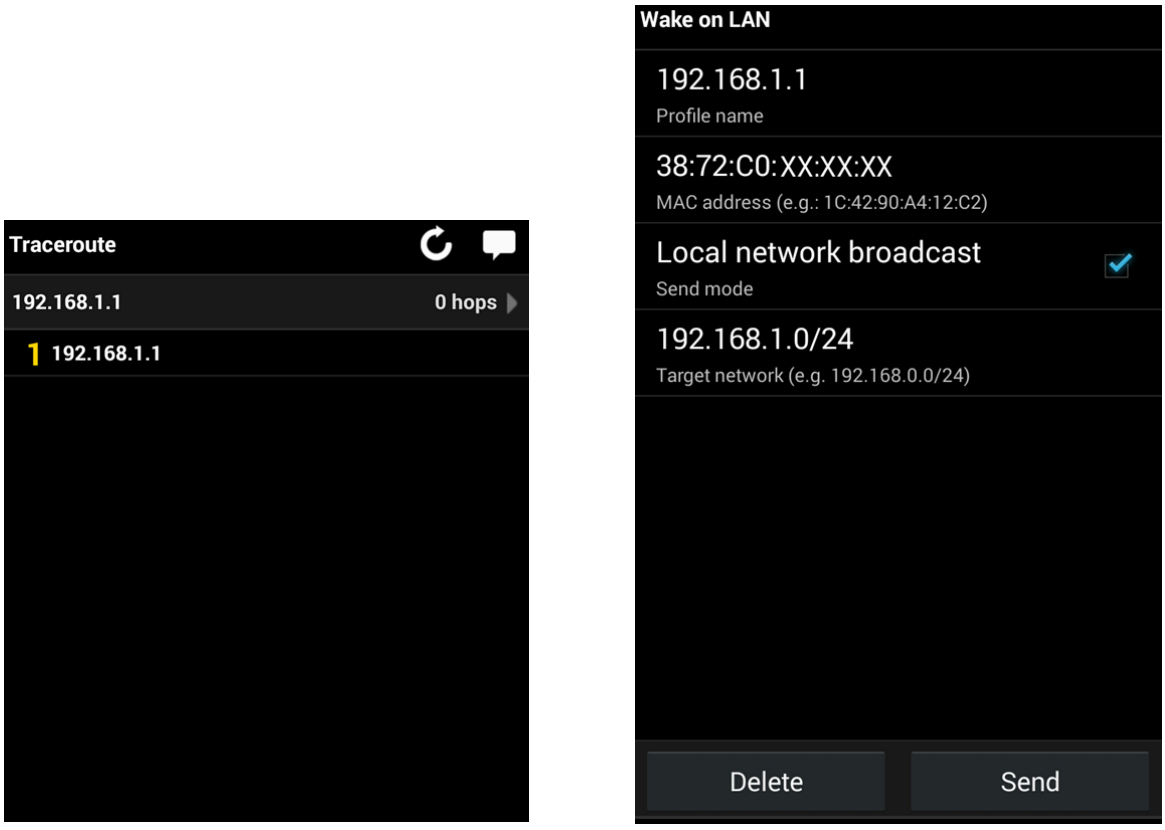


Figura 19. *Fing*: Traceroute y Wake on Lan

CAPÍTULO IV

DISEÑO

IV. DISEÑO

En este capítulo se realiza un estudio sobre una herramienta de análisis de redes junto con una descripción del diseño del sistema a desarrollar, a partir de dicho estudio.

4.1. Funcionamiento de herramientas existentes

Para estudiar el funcionamiento de una herramienta de análisis de redes se ha elegido la aplicación *Fing* entre otras como *Net Analyzer*, *IP Scanner* o *iNet*, ya que era la que más se ajustaba en cuanto a uso y funcionamiento a nuestro objetivo.

4.1.1. Escenario

La red a escanear para realizar el estudio es la red Ethernet del laboratorio 4.1.F04 del edificio Torres Quevedo. Se ha elegido esta red por ser una red pequeña y así analizar con mayor claridad el intercambio de mensajes.

Una vez asociado el smartphone al AP, el dispositivo pertenece a la red del laboratorio y el escenario resultante se puede ver en la Figura 20.

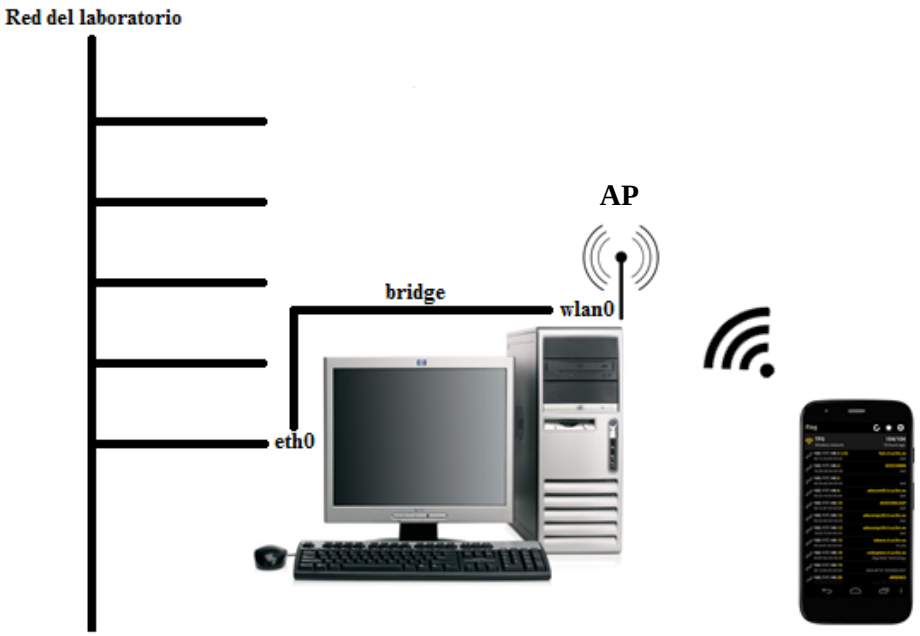


Figura 20. Escenario análisis

4.1.2. Ejecución

Para conocer el funcionamiento de la aplicación, necesitamos capturar el intercambio de mensajes que se realiza mientras se está ejecutando el escaneo de la red. Utilizaremos la herramienta de captura Wireshark, la cual permite capturar los paquetes que se han intercambiado durante un experimento.

Con el smartphone conectado a la red como se ha explicado en el punto anterior, lanzamos la aplicación *Fing* para que realice el escaneo de la red. El resultado se puede ver en la Figura 21:

Figura 21. Escaneo "TFG"

Al mismo tiempo que ejecutamos la aplicación, iniciamos una nueva captura en Wireshark en el interfaz wlan0, filtrando la dirección MAC del smartphone para comprobar qué mensajes se intercambian durante el escaneo.

No.	Time	Source	Destination	Protocol	Info
72	1.193064	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.1? Tell 163.117.140.36
73	1.193064	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.1? Tell 163.117.140.36
79	1.206222	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.3? Tell 163.117.140.36
80	1.206222	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.3? Tell 163.117.140.36
87	1.225748	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.5? Tell 163.117.140.36
88	1.225747	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.5? Tell 163.117.140.36
89	1.225994	Dell_5a:9e:fe	34:bb:26:[illegible]	ARP	163.117.140.5 is at 00:23:ae:5a:9e:fe
92	1.236534	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.6? Tell 163.117.140.36
93	1.236533	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.6? Tell 163.117.140.36
94	1.236766	Dell_52:57:53	34:bb:26:[illegible]	ARP	163.117.140.6 is at 00:22:19:52:57:53
97	1.246321	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.7? Tell 163.117.140.36
98	1.246320	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.7? Tell 163.117.140.36
99	1.256512	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.8? Tell 163.117.140.36
100	1.256511	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.8? Tell 163.117.140.36
101	1.266929	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.9? Tell 163.117.140.36
102	1.266928	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.9? Tell 163.117.140.36
105	1.287411	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.11? Tell 163.117.140.36
106	1.287409	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.11? Tell 163.117.140.36
107	1.297661	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.12? Tell 163.117.140.36
108	1.297660	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.12? Tell 163.117.140.36
109	1.297895	Dell_5a:a4:f0	34:bb:26:[illegible]	ARP	163.117.140.12 is at 00:23:ae:5a:a4:f0
113	1.309042	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.13? Tell 163.117.140.36
114	1.309041	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.13? Tell 163.117.140.36
115	1.309593	18:03:73:d3:11:09	34:bb:26:[illegible]	ARP	163.117.140.13 is at 18:03:73:d3:11:09
118	1.319805	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.14? Tell 163.117.140.36
119	1.319804	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.14? Tell 163.117.140.36
123	1.330401	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.15? Tell 163.117.140.36
124	1.330400	34:bb:26:[illegible]	Broadcast	ARP	Who has 163.117.140.15? Tell 163.117.140.36

Figura 22. Captura ARP Wireshark escaneo "TFG"

No.	Time	Source	Destination	Protocol	Info
608	2.536490	163.117.140.36	163.117.140.166	DNS	Standard query PTR 46.140.117.163.in-addr.arpa
609	2.536921	163.117.140.166	163.117.140.36	DNS	Standard query response PTR mosquito.it.uc3m.es
612	2.541379	163.117.140.36	163.117.140.166	DNS	Standard query PTR 51.140.117.163.in-addr.arpa
613	2.541815	163.117.140.166	163.117.140.36	DNS	Standard query response PTR leone.it.uc3m.es
614	2.543674	163.117.140.36	163.117.140.166	DNS	Standard query PTR 71.140.117.163.in-addr.arpa
615	2.544006	163.117.140.166	163.117.140.36	DNS	Standard query response PTR larva10.it.uc3m.es
616	2.549091	163.117.140.36	163.117.140.166	DNS	Standard query PTR 76.140.117.163.in-addr.arpa
617	2.549494	163.117.140.166	163.117.140.36	DNS	Standard query response PTR catarina.it.uc3m.es
618	2.551261	163.117.140.36	163.117.140.166	DNS	Standard query PTR 81.140.117.163.in-addr.arpa
619	2.551603	163.117.140.166	163.117.140.36	DNS	Standard query response PTR viudanegra.it.uc3m.es
620	2.553598	163.117.140.36	163.117.140.166	DNS	Standard query PTR 4.140.117.163.in-addr.arpa
621	2.553979	163.117.140.166	163.117.140.36	DNS	Standard query response PTR adscom00.it.uc3m.es
622	2.555728	163.117.140.36	163.117.140.166	DNS	Standard query PTR 96.140.117.163.in-addr.arpa
623	2.556027	163.117.140.166	163.117.140.36	DNS	Standard query response, No such name
624	2.557884	163.117.140.36	163.117.140.166	DNS	Standard query PTR 101.140.117.163.in-addr.arpa
625	2.558259	163.117.140.166	163.117.140.36	DNS	Standard query response PTR sapo.it.uc3m.es
626	2.560254	163.117.140.36	163.117.140.166	DNS	Standard query PTR 19.140.117.163.in-addr.arpa
627	2.560552	163.117.140.166	163.117.140.36	DNS	Standard query response, No such name
628	2.562552	163.117.140.36	163.117.140.166	DNS	Standard query PTR 106.140.117.163.in-addr.arpa
629	2.562887	163.117.140.166	163.117.140.36	DNS	Standard query response PTR zapatero.it.uc3m.es
630	2.564641	163.117.140.36	163.117.140.166	DNS	Standard query PTR 111.140.117.163.in-addr.arpa
631	2.565058	163.117.140.166	163.117.140.36	DNS	Standard query response PTR krill.it.uc3m.es
632	2.567748	163.117.140.36	163.117.140.166	DNS	Standard query PTR 116.140.117.163.in-addr.arpa
633	2.568089	163.117.140.166	163.117.140.36	DNS	Standard query response PTR percebe.it.uc3m.es
636	2.570078	163.117.140.36	163.117.140.166	DNS	Standard query PTR 121.140.117.163.in-addr.arpa
637	2.570382	163.117.140.166	163.117.140.36	DNS	Standard query response, No such name
638	2.572140	163.117.140.36	163.117.140.166	DNS	Standard query PTR 44.140.117.163.in-addr.arpa
639	2.572492	163.117.140.166	163.117.140.36	DNS	Standard query response, No such name

Figura 23. Captura DNS Wireshark escaneo "TFG"

Como se puede ver en la Figura 22, *Fing* realiza peticiones broadcast ARP para averiguar qué direcciones IP han sido asignadas dentro de la red. Se sabrá que una dirección no ha sido asignada si pasado el timeout no ha habido respuesta.

Con este mecanismo *Fing* puede averiguar todos los dispositivos que están conectados a la red, sabiendo su dirección IP y su dirección MAC.

Para conocer el nombre de la máquina realiza peticiones DNS a cada dirección IP que pertenece a la red (Figura 23). El protocolo DNS [14] [15] es un sistema de nomenclatura jerárquica, asocia información variada con nombres de dominio. Su función es traducir identificadores binarios de los equipos conectados a la red a nombres inteligibles. Existen varios tipos de registros DNS para obtener información sobre el servidor DNS primario de la zona, los servidores de correo o traducir nombres de servidores a direcciones IP.

En este caso, *Fing* realiza peticiones DNS de tipo PTR, también conocido como registro inverso; que traduce direcciones IP en nombres de dominio, usando el archivo de configuración de la zona DNS inversa. La aplicación realiza peticiones de tipo PTR a todas las direcciones IP conectadas a la red.

Como se puede ver en algunas respuestas (*"No such name"*) todas las máquinas no tienen asignadas un nombre.

4.2. Arquitectura del sistema

En este apartado se define la estructura que tendrá el sistema a desarrollar. En la siguiente figura se puede observar un esquema general:

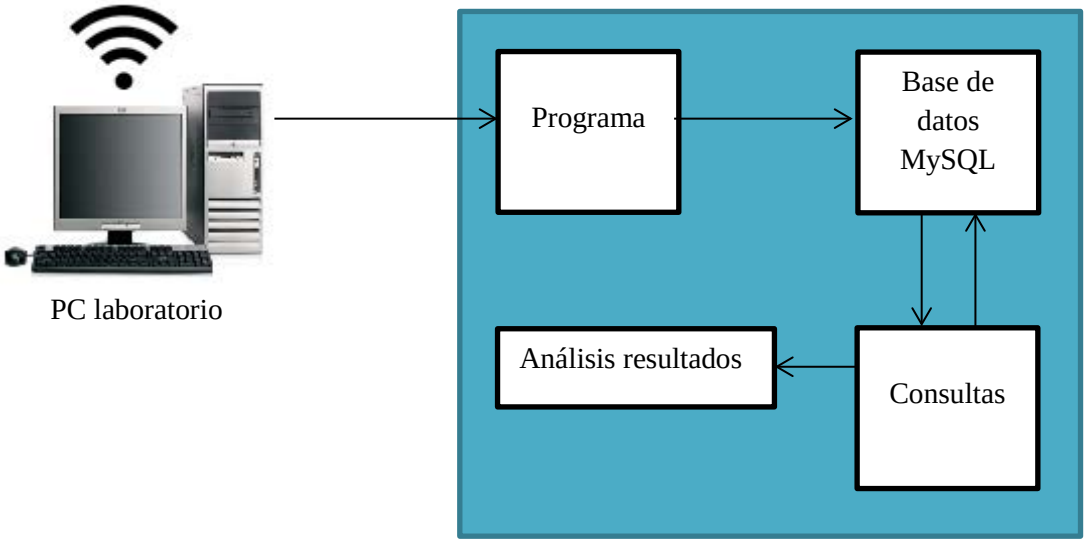


Figura 24. Arquitectura del sistema

Como se puede ver en el esquema de la Figura 24, el sistema consta de cinco partes fundamentales:

- **PC laboratorio:** conectado a la red inalámbrica a escanear.
- **Programa:** encargado de realizar escaneos periódicos.
- **Base de datos MySQL:** donde se almacenará toda la información.
- **Consultas:** se realizarán diversas consultas para su posterior análisis.
- **Análisis resultados:** se analizarán gráficamente los resultados obtenidos.

4.3. Programa

Para el diseño del programa nos basaremos en el funcionamiento de *Fing*, analizado en el apartado 4.1.

Como hemos visto necesitamos disponer de un cliente ARP para detectar los usuarios que se conectan a la red. Para ello utilizaremos como base el cliente ARP diseñado en la asignatura Redes y Servicios de Comunicaciones Avanzadas como parte del desarrollo de un demonio RIPv2. En las especificaciones de este cliente ARP se pedía desarrollar un programa basado en la librería *librawnet* [16], y las implementaciones base de los protocolos Ethernet e IPv4, que mostrase por pantalla la dirección MAC asociada a la dirección IPv4 que se pasa como parámetro, junto con el interfaz que se desea emplear.

La librería *librawnet* facilitada permite acceder directamente a los interfaces de red del equipo, está diseñada para la programación de protocolos "en crudo". Los paquetes enviados y recibidos no han sido procesados por la pila de protocolos del equipo, por lo que es necesario añadir y procesar las cabeceras de todos los protocolos de la pila que se desea desarrollar. Realmente el kernel y *librawnet* reciben una copia de todos los paquetes recibidos por la tarjeta de red. *Librawnet* proporciona dos módulos: temporizadores con precisión de milisegundos y gestión de los interfaces de red.

Para el envío y recepción de mensajes es necesario crear una estructura con los campos de la cabecera ARP como se puede ver en la Figura 25:

```
struct struct_arp{

        uint16_t dir_type_hardware;
        uint16_t dir_type_protocol;
        uint8_t length_MAC;
        uint8_t length_IP;
        uint16_t opcode;
        mac_addr_t mac_org_arp;
        ipv4_addr_t ip_addr_org;
        mac_addr_t mac_dst_arp;
        ipv4_addr_t ip_addr_dst;

};
```

Figura 25. Estructura cabecera ARP

Estos datos se envían en una trama Ethernet con dirección de destino FF:FF:FF:FF:FF:FF (broadcast) y tipo 0x806 (ARP) por el interfaz deseado.

Para recibir la respuesta nos mantenemos a la espera durante el timeout establecido hasta que lleguen datos por dicho interfaz. Al llegar el mensaje comprobamos que se trata de un *arp reply* (código de operación: 0x0002) y que la dirección IP del emisor corresponde con la dirección IP pedida en el *arp request*. Si los datos son correctos, obtenemos la dirección MAC correspondiente a la dirección IP.

En nuestro caso no vamos a pedir la dirección MAC de una única dirección IP, por lo que el cliente ARP tiene varias modificaciones.

En primer lugar el único parámetro que necesita es el interfaz que se desea emplear para escanear la red a la que está conectado. La dirección IP origen la obtenemos mediante el uso de sockets, junto con la máscara de red. Con estos dos datos podemos obtener cuál es la primera dirección IP por la que debemos preguntar. También podemos obtener el prefijo de la red para saber el número total de dispositivos que se pueden conectar a la red.

Dependiendo del tamaño de la red, realizar las peticiones a todos las direcciones IP que puedan estar conectadas puede tardar demasiado tiempo para llevar un seguimiento adecuado. Por este motivo se realizaron dos tipos de clientes ARP en función de la manera en que se realizan las peticiones.

4.3.1. Peticiones en secuencia

En el primer cliente ARP, las peticiones se realizarán en secuencia, es decir, una a una. Esto se debe a que se quiere testear el buen funcionamiento del programa en la red del laboratorio, escaneando en el interfaz eth0, puesto que la red es pequeña. El funcionamiento de este cliente ARP es sencillo. Se mandan peticiones a cada dirección de la red en secuencia hasta que se preguntan por todas las posibles, cuando se vuelve a repetir el proceso. El tiempo máximo de espera es de 100ms; si pasado ese tiempo no se recibe respuesta, se supone que esa dirección no está asignada y se pregunta por la siguiente.

Una vez que comprobamos que los resultados son los mismos que si lanzamos la aplicación *Fing* a la vez, vemos que el funcionamiento es correcto. Por lo tanto cada vez que obtenemos un nuevo usuario, almacenamos su información en la base de datos.

El siguiente paso es probar el funcionamiento en una red más grande y escaneando en el interfaz inalámbrico. De las dos redes inalámbricas disponibles (*WiFi-UC3M* y *eduroam*) comenzamos probando el programa en *eduroam*.

Para conectarse a *eduroam* es necesario instalar el paquete *wpa_supplicant*, que es el componente IEEE 802.1X/WPA utilizado por las estaciones cliente. Implementa las negociaciones entre la clave y un WPA Authenticator, controlando la asociación y autenticación [17]. Para lanzar el *wpa_supplicant* y poder asociarnos a *eduroam*, necestiamos configurar al archivo *wpa_supplicant.conf* de la siguiente manera:

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
eapol_version=1

network={
    ssid="eduroam"
    key_mgmt=WPA-EAP
    proto=WPA2 WPA
    eap=TTLS
    pairwise=CCMP TKIP
    identity="nia@alumnos.uc3m.es"
    password="password"
    priority=2
    phase2="auth=MSCHAPV2"
}
```

Figura 26. Archivo configuración *wpa_supplicant*

Al lanzar el *wpa_supplicant* con la configuración mencionada, nos asociaremos a *eduroam* (Figura 27), pero aún no tendremos una dirección IP en la red. Para ello hacemos uso del cliente DHCP, pidiendo una dirección IP en el interfaz inalámbrico wlan0.

```
Trying to associate with 00:27:0d:56:01:61 (SSID='eduroam' freq=2462 MHz)
Associated with 00:27:0d:56:01:61
CTRL-EVENT-EAP-STARTED EAP authentication started
CTRL-EVENT-EAP-METHOD EAP vendor 0 method 21 (TTLS) selected
EAP-TTLS: Phase 2 MSCHAPV2 authentication succeeded
CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
WPA: Key negotiation completed with 00:27:0d:56:01:61 [PTK=CCMP GTK=TKIP]
CTRL-EVENT-CONNECTED - Connection to 00:27:0d:56:01:61 completed (auth) [id=0 id_str=]
```

Figura 27. Asociación a *eduroam*

Con el PC del laboratorio conectado a *eduroam* podemos probar nuestro cliente ARP para testear su funcionamiento.

El funcionamiento del programa es correcto, pero al cabo de las ejecuciones no permite realizar más peticiones. Esto es debido a la seguridad que posee *eduroam*, que al advertir demasiadas peticiones broadcast ARP, deniega la posibilidad de continuar mandando peticiones, para evitar posibles ataques de inundación en la red.

Por lo tanto la red inalámbrica elegida para realizar los escaneos y posteriores análisis será *WiFi-UC3M*. Al ser una red abierta no precisa de ningún tipo de

credenciales, por lo que con conectarse y pedir una dirección IP mediante DHCP es suficiente.

En *WiFi-UC3M* el programa sigue funcionando según lo esperado, monitorizando la red durante un mes. El problema de esta red es que es mayor que *eduroam*; *WiFi-UC3M* posee un prefijo /16, lo que implica 65536 posibles direcciones para los hosts, mientras que *eduroam* posee un prefijo /20 o 4096 posibles hosts. Esto implica que para realizar un escaneo completo de la red realizando las peticiones en secuencia se emplea demasiado tiempo, aproximadamente 50 minutos de media, dependiendo del número de usuarios conectados. Con tanto tiempo entre cada escaneo no se pueden obtener datos concluyentes.

4.3.2. Peticiones en paralelo

En el segundo cliente ARP se realizarán las peticiones en paralelo, es decir, mediante ráfagas. Esto se debe a que se quiere testear el buen funcionamiento del programa en *WiFi-UC3M*, escaneando en wlan0, una red grande que requiere un tiempo de escaneo menor.

Para disminuir el tiempo de duración del escaneo, tanto el envío como la recepción de peticiones se realizan mediante hilos. Para ello el hilo de envío manda peticiones en ráfagas de X direcciones cada X ms, mientras que el hilo de recepción se queda a la espera de recibir tramas dentro de los 100 ms del timeout.

Variando el número de direcciones por ráfaga, el tiempo total aproximado en realizar un escaneo completo de la red sería el siguiente:

Número de peticiones	Tiempo(ms)/ráfaga	Tiempo total de escaneo
128	500	4’15’’
64	500	8’30’’
32	500	17’
16	500	34’10’’

Tabla 2. Variación ráfagas

El objetivo es realizar escaneos cada 5 o 10 minutos para realizar un buen seguimiento de los usuarios. Teniendo en cuenta los resultados anteriores optaríamos por mandar ráfagas de 128 o 64 peticiones cada 500 ms. El problema de la primera opción es que son demasiadas peticiones para que el hilo de recepción pueda ser capaz de obtener todas las respuestas, por lo que se podrían perder datos. Por lo tanto se ha decidido enviar peticiones en ráfagas de 64 direcciones cada 500ms.

Para llevar un seguimiento constante se realizará un escaneo completo de la red cada 10 min, aunque el tiempo total de escaneo sea algo menor.

Con esta configuración y con el correspondiente almacenamiento de los datos obtenidos en la base de datos, el funcionamiento del programa es el previsto.

4.4. Base de datos MySQL

SQL (*Structed Query Language*) es un lenguaje de acceso a bases de datos relacionales muy popular y su estandarización hace bastante más fácil almacenar, actualizar y procesar datos. MySQL es un sistema de gestión de bases de datos relacional, multiusuario y multihilo de código abierto. Sus principales características son [18]:

- Permite ser usado a través de varios lenguajes: C, C++, Java, PHP, Python.
- Disponibilidad en gran cantidad de plataformas y sistemas.
- Cuenta con un sistema de privilegios y contraseñas.
- Permite el uso simultáneo de varias CPU.
- Transacciones y claves foráneas.
- Manejo del álgebra y el cálculo relacional.

Para almacenar los datos obtenidos del programa se han creado las siguientes tablas:

- Tabla Direcciones: almacena información sobre cada usuario encontrado.

```
+-------------+-------------+------+-----+-------------------+-----------------------------+
| Field       | Type        | Null | Key | Default           | Extra                       |
+-------------+-------------+------+-----+-------------------+-----------------------------+
| id          | int(11)     | NO   | PRI | NULL              | auto_increment              |
| IP_address  | varchar(15) | NO   |     | NULL              |                             |
| MAC_address | varchar(17) | NO   |     | NULL              |                             |
| RTTms       | int(11)     | NO   |     | NULL              |                             |
| Ejecucion   | int(11)     | NO   |     | NULL              |                             |
| Time        | timestamp   | NO   |     | CURRENT_TIMESTAMP | on update CURRENT_TIMESTAMP |
+-------------+-------------+------+-----+-------------------+-----------------------------+
```

Figura 28. MySQL: Descripción tabla Direcciones

En la siguiente figura se puede ver un ejemplo de cómo se almacenan los datos al registrar cada usuario nuevo:

- **id:** identificador único de cada entrada.
- **IP_address:** dirección IP del usuario.
- **MAC_address:** dirección MAC del usuario.

- **RTTms:** RTT de la petición.
- **Ejecución:** número de ejecución asociado a cada escaneo.
- **Time:** fecha y hora en la que se ha realizado la petición.

id	IP_address	MAC_address	RTTms	Ejecucion	Time
1	10.100.0.2	00:0D:66:17:98:1A	5	1	2015-01-22 19:10:01
2	10.100.0.3	64:00:F1:7F:6C:6B	5	1	2015-01-22 19:10:01
3	10.100.0.8	30:E4:DB:38:A7:0F	5	1	2015-01-22 19:10:01
4	10.100.0.7	30:E4:DB:38:A0:0F	5	1	2015-01-22 19:10:01
5	10.100.0.6	00:1D:45:BB:AB:0B	5	1	2015-01-22 19:10:01
6	10.100.0.5	00:1D:45:B9:B1:AB	6	1	2015-01-22 19:10:01
7	10.100.0.4	64:00:F1:7F:A6:EB	9	1	2015-01-22 19:10:01
8	10.100.3.230	88:32:9B:68:E2:18	23	1	2015-01-22 19:10:08
9	10.100.15.137	BC:85:1F:49:3F:D7	32	1	2015-01-22 19:10:32
10	10.100.17.32	CC:FA:00:DB:FA:62	17	1	2015-01-22 19:10:35
11	10.100.28.69	18:CF:5E:73:A9:92	14	1	2015-01-22 19:10:57
12	10.100.28.182	44:D4:E0:56:39:56	60	1	2015-01-22 19:10:58
13	10.100.30.180	3C:E0:72:E5:68:12	41	1	2015-01-22 19:11:02
14	10.100.34.120	2C:44:FD:BE:7C:7B	36	1	2015-01-22 19:11:09
15	10.100.35.201	08:ED:B9:E7:C4:1B	12	1	2015-01-22 19:11:12
16	10.100.40.34	FC:25:3F:B4:65:9F	37	1	2015-01-22 19:11:21
17	10.100.40.153	00:08:22:0D:22:2E	6	1	2015-01-22 19:11:22
18	10.100.42.25	EC:35:86:85:11:7B	8	1	2015-01-22 19:11:25
19	10.100.42.107	84:38:35:C8:90:25	28	1	2015-01-22 19:11:25
20	10.100.44.18	60:6C:66:23:BC:8E	14	1	2015-01-22 19:11:29

Figura 29. MySQL: Ejemplo tabla Direcciones

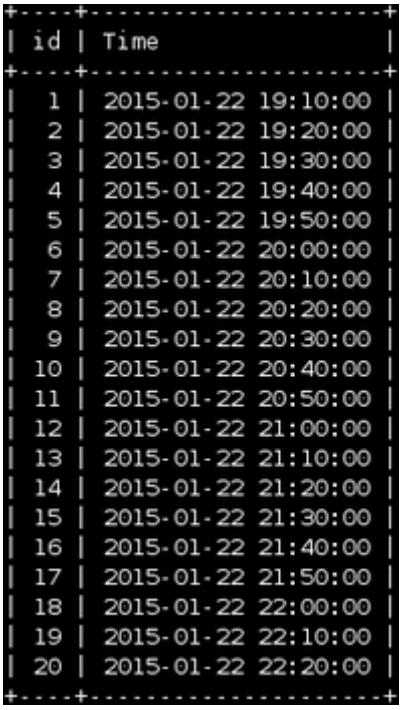
- Tabla Ejecuciones: almacena el tiempo en que se realiza cada escaneo.

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	
Time	timestamp	NO		CURRENT_TIMESTAMP	on update CURRENT_TIMESTAMP

Figura 30. MySQL: Descripción tabla Ejecuciones

En la siguiente figura se puede ver un ejemplo de cómo se almacenan los datos al realizar cada escaneo:

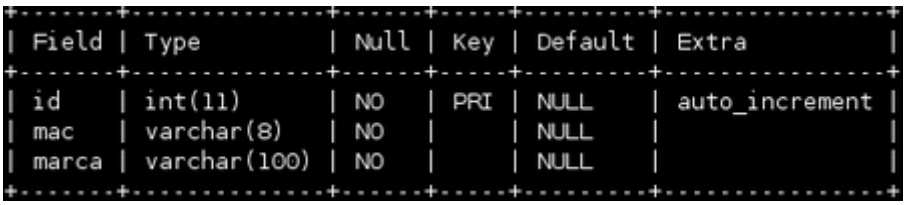
- **id:** identificador único de cada entrada.
- **Time:** fecha y hora en la que se ha realizado el escaneo.



id	Time
1	2015-01-22 19:10:00
2	2015-01-22 19:20:00
3	2015-01-22 19:30:00
4	2015-01-22 19:40:00
5	2015-01-22 19:50:00
6	2015-01-22 20:00:00
7	2015-01-22 20:10:00
8	2015-01-22 20:20:00
9	2015-01-22 20:30:00
10	2015-01-22 20:40:00
11	2015-01-22 20:50:00
12	2015-01-22 21:00:00
13	2015-01-22 21:10:00
14	2015-01-22 21:20:00
15	2015-01-22 21:30:00
16	2015-01-22 21:40:00
17	2015-01-22 21:50:00
18	2015-01-22 22:00:00
19	2015-01-22 22:10:00
20	2015-01-22 22:20:00

Figura 31. MySQL: Ejemplo tabla Ejecuciones

- Tabla Marcas: almacena rangos de direcciones MAC con su correspondiente marca.



Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	auto_increment
mac	varchar(8)	NO		NULL	
marca	varchar(100)	NO		NULL	

Figura 32. MySQL: Descripción tabla Marcas

En la siguiente figura se puede ver un ejemplo de las marcas almacenadas, obtenidas en [19]:

- **id:** identificador único de cada entrada.
- **mac:** rango de dirección MAC.
- **marca:** marca del dispositivo.

id	mac	marca
1	00:00:00	XEROX CORPORATION
2	00:00:01	XEROX CORPORATION
3	00:00:02	XEROX CORPORATION
4	00:00:03	XEROX CORPORATION
5	00:00:04	XEROX CORPORATION
6	00:00:05	XEROX CORPORATION
7	00:00:06	XEROX CORPORATION
8	00:00:07	XEROX CORPORATION
9	00:00:08	XEROX CORPORATION
10	00:00:09	XEROX CORPORATION
11	00:00:0A	OMRON TATEISI ELECTRONICS CO.
12	00:00:0B	MATRIX CORPORATION
13	00:00:0C	CISCO SYSTEMS, INC.
14	00:00:0D	FIBRONICS LTD.
15	00:00:0E	FUJITSU LIMITED
16	00:00:0F	NEXT, INC.
17	00:00:10	SYTEK INC.
18	00:00:11	NORMEREL SYSTEMES
19	00:00:12	INFORMATION TECHNOLOGY LIMITED
20	00:00:13	CAMEX

Figura 33. MySQL: Ejemplo tabla Marcas

Esta tabla se utilizará en las consultas para realizar análisis relativos a las marcas de los dispositivos.

CAPÍTULO V

ANÁLISIS RESULTADOS

V. ANÁLISIS RESULTADOS

En este capítulo se realiza un análisis de los resultados obtenidos por el programa. Para ello se creará un programa que, mediante consultas a la información almacenada en la base de datos, obtenga los datos para su posterior análisis.

Para la realización de los gráficos se ha utilizado la herramienta Web *Highcharts* [20], ya que ofrece un método fácil e interactivo para insertar gráficas.

En la siguiente tabla se pueden ver algunos datos relevantes sobre el total de la captura:

Inicio	2015-01-23 00:00
Fin	2015-02-19 23:50
Duración	4 semanas
Escaneos	4 032
Entradas	2 234 658
Usuarios	26 017
Media usuarios/escaneo	554
Media usuarios/día	4 500
Media RTT(ms)	24,94

Tabla 3. Datos totales de la captura

A continuación se van a mostrar gráficos sobre distintos aspectos a tener en cuenta en el total de la captura:

En la Figura 34 se puede ver el número de usuarios encontrados en cada escaneo (cada 10 min).

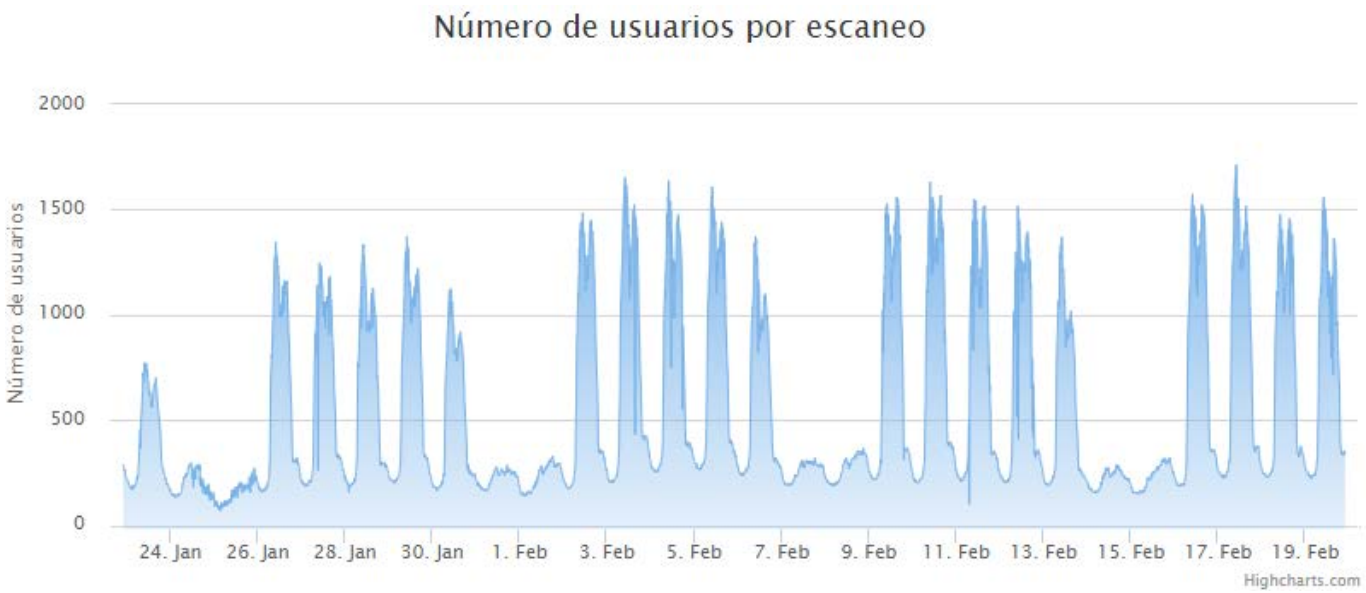


Figura 34. Usuarios por escaneo

En la Figura 35 se puede ver el número de usuarios que se han conectado cada día a la red. Se puede apreciar con claridad el decremento de usuarios los fines de semana.

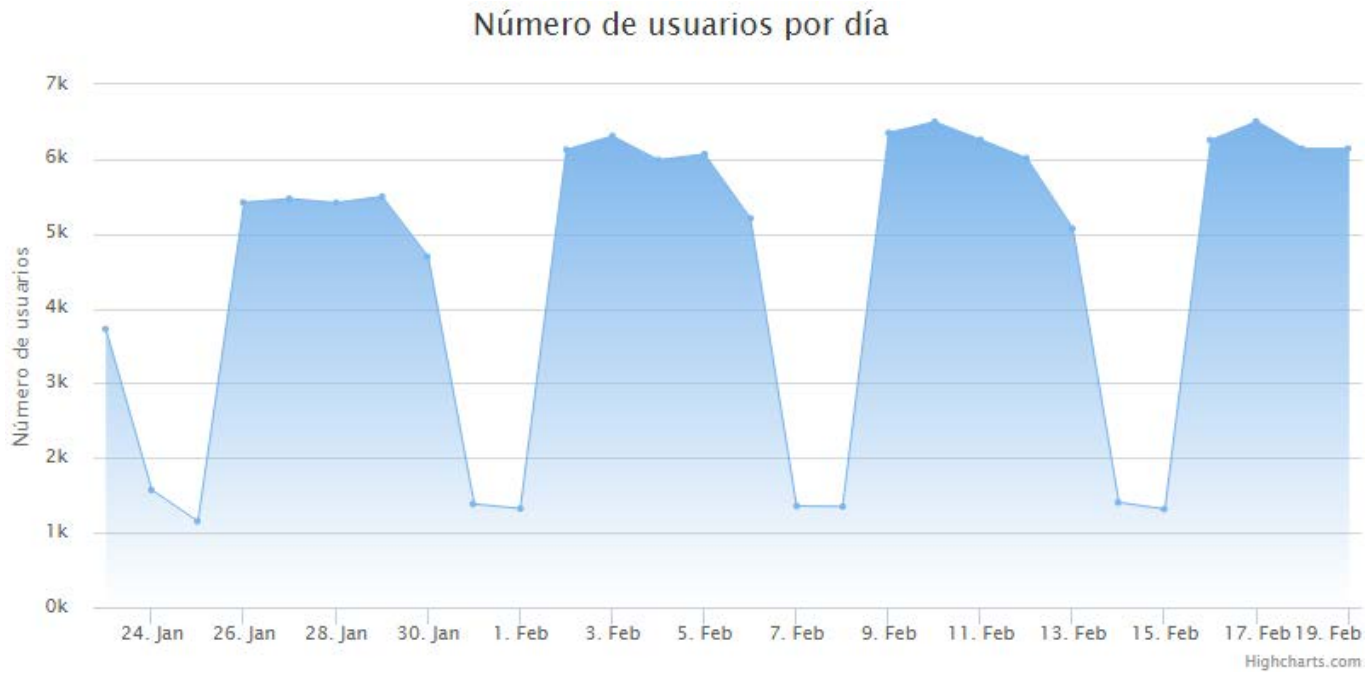


Figura 35. Usuarios por día

En la siguiente tabla se pueden ver las marcas de los dispositivos de los usuarios encontrados durante el total de la captura:

Marca	Usuarios	Porcentaje
Apple	6 504	25%
Otros	4 412	17%
Samsung	3 850	14,8%
Sony	2 107	8,1%
LG	1 769	6,8%
Hon Hai	1 535	5,9%
Intel	1 092	4,2%
Murata Manufactuaring	884	3,4%
Huawei	780	3%
Liteon	780	3%
BQ	702	2,7%
Motorola	520	2%
InPro	494	1,9%
HTC	338	1,3%
Clipcomm	260	1%

Tabla 4. Marcas de dispositivos

En la Figura 36 se pueden ver el número de usuarios que se conectan cada hora a la red, comparándose cada día de la semana:

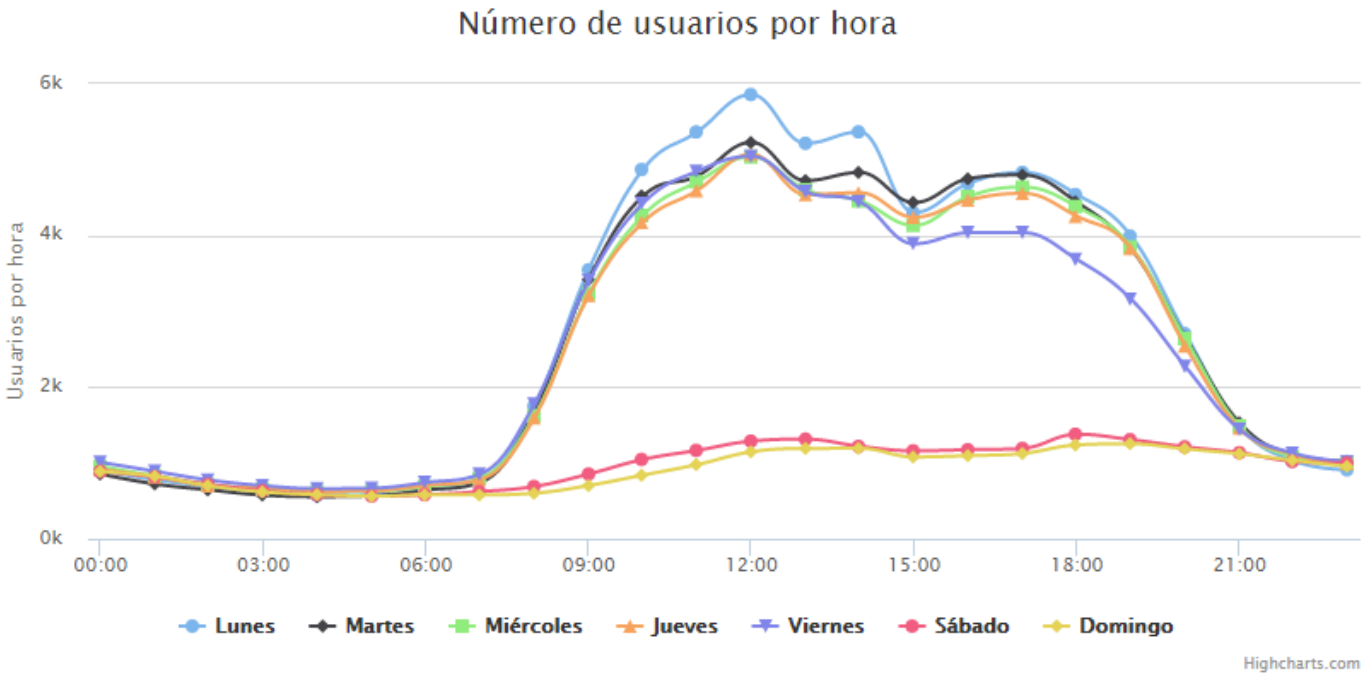


Figura 36. Usuarios por hora (semana)

Teniendo en cuenta los datos sobre el número de usuarios que se conectan cada hora los sábados y domingos, se podría intentar deducir qué ordenadores son fijos.

Se podría decir que existen alrededor de 700 ordenadores fijos conectados a la red *WiFi-UC3M*.

Con los datos almacenados también se podrían hacer seguimientos individuales de los usuarios. En la Figura 40 hemos seleccionado 5 usuarios de forma aleatoria para analizar sus patrones de conectividad, registrando el tiempo de estancia en horas que permanece conectados cada día a la red:

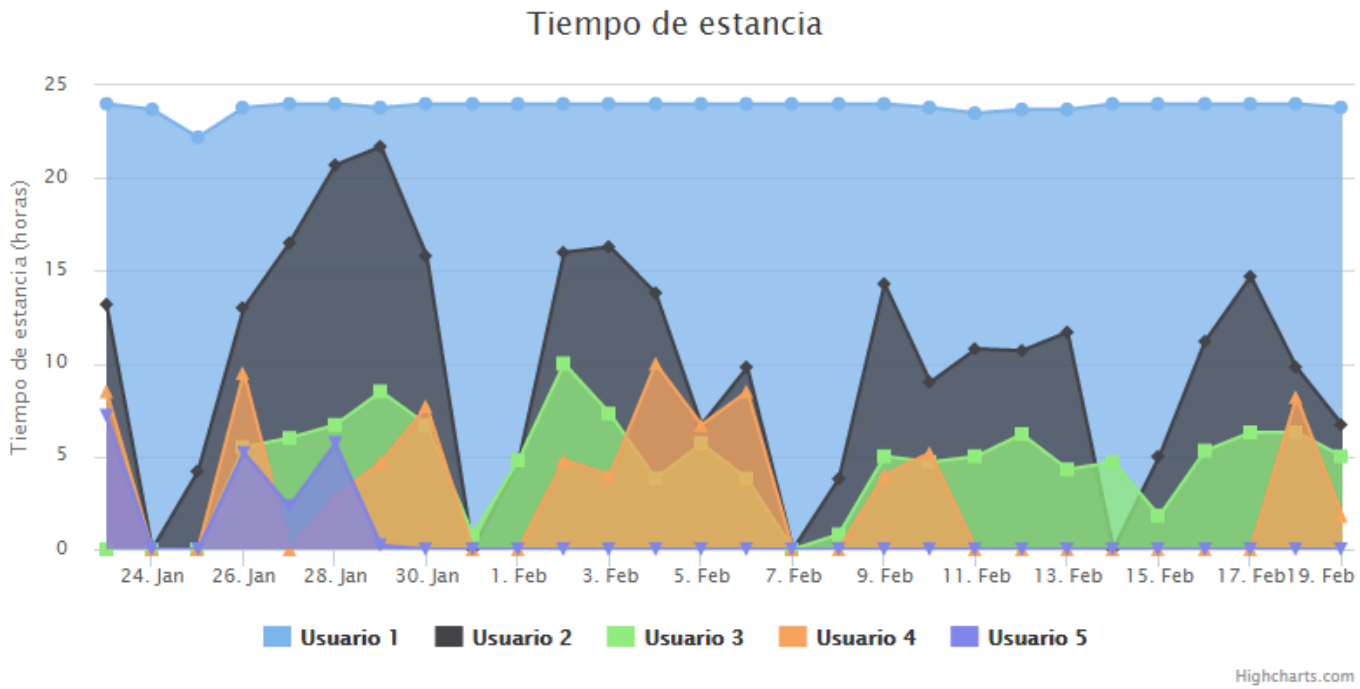


Figura 37. Tiempo de estancia usuarios

En esta figura se puede apreciar claramente distintos patrones de conectividad. El Usuario 1 probablemente sea un ordenador fijo, el cual siempre está conectado a la red. El Usuario 2 también puede que sea un ordenador fijo o portátil, aunque no está siempre conectado a la red, por lo que su conexión a la red puede que dependa de su uso. En cuanto a los usuarios 3 y 4 parecen dispositivos móviles, de alumnos o profesores, con un patrón de conectividad adecuado al horario lectivo. Del Usuario 5 no se pueden sacar muchas conclusiones ya que no aparece con mucha frecuencia.

La realización de análisis más detallados, como poder hacer una clasificación más ajustada del tipo de usuario en función de su comportamiento y marca del dispositivo, es trabajo futuro de otro Trabajo Fin de Grado en curso.

CAPÍTULO VI

CONCLUSIONES Y TRABAJOS FUTUROS

VI. CONCLUSIONES Y TRABAJOS FUTUROS

En este capítulo se presentan las conclusiones obtenidas tras la finalización del Trabajo de Fin de Grado, así como una serie de posibles trabajos futuros en base a este proyecto.

6.1. Conclusiones

En este Trabajo Fin de Grado se pretendía desarrollar un sistema capaz de escanear una red inalámbrica del campus de la Universidad Carlos III de Madrid de forma periódica para analizar la conectividad de sus usuarios.

El primer paso para el desarrollo del sistema fue realizar un estudio de alguna herramienta de análisis de redes para conocer su funcionamiento y poder implementar un programa en función a sus características. La herramienta elegida para el estudio fue la aplicación Fing.

Una vez realizado el estudio, se procedió a la implementación del código. En la primera implementación de las peticiones en secuencia, el tiempo entre cada escaneo no era el adecuado para llevar un seguimiento significativo de la conectividad. En la segunda implementación de las peticiones en paralelo se consiguió obtener un tiempo ajustable entre escaneos, dependiendo del número de peticiones que se realizasen en cada ráfaga. Con este mecanismo conseguimos realizar escaneos cada 10 minutos, llevando un seguimiento significativo de la conectividad.

Desplegado ya el sistema, se dejó monitorizando durante un período amplio de tiempo como para hacer un estudio sobre la red. Para ello se realizó un análisis de los resultados, accediendo a la información almacenada en la base de datos, mostrando mediante gráficos distintos aspectos sobre la conectividad de los usuarios.

Finalmente se puede decir que se han alcanzado todos los objetivos propuestos en este Trabajo Fin de Grado, comprobando con los resultados obtenidos que el sistema cumple con los requisitos planteados y que puede ser utilizado para realizar una gestión eficiente de la red.

6.2. Trabajos futuros

A continuación se enumeran algunas futuras mejoras del sistema implementado o posibles cambios:

- **Mejora del programa:** Puesto que la eficacia del sistema depende del intervalo de tiempo en que se realiza cada escaneo, se podría intentar monitorizar la red cada 5 min, o dentro del mismo escaneo hacer un seguimiento sólo de los usuarios que están conectados.

- **Monitorización en *eduroam*:** Sería interesante realizar una monitorización en la red *eduroam*, ya que de momento el programa no funciona en dicha red. Se están investigando las causas con el personal de servicios informáticos.

- **Período amplio de tiempo:** La idea inicial del Trabajo Fin de Grado es continuar con los análisis de la red durante un cuatrimestre al menos, para así tener datos más concluyentes.

- **Implementación Web:** Implementación de una aplicación Web donde se puedan realizar consultas en tiempo real.

- **Asistencia:** Manteniendo la monitorización durante un período amplio de tiempo, se podrían realizar análisis sobre asistencia mediante la integración de horarios de clase.

- **Localización:** Escaneando la red en sus diferentes subredes y conociendo la localización y el rango de cobertura de cada una de ellas, podrían realizarse mapas de calor con el movimiento de los usuarios dentro de la red.

- **Análisis detallados:** La realización de análisis más detallados es trabajo futuro de otro Trabajo Fin de Grado en curso.

CAPÍTULO VII

CONCLUSIONS AND FUTURE WORKS

VII. CONCLUSIONS AND FUTURE WORKS

In this chapter the conclusions obtained after concluding the Bachelor Thesis are presented, as well as a range of possible future work based on this project.

7.1. Conclusions

This Bachelor Thesis was intended to develop a system capable of scanning a wireless campus network of the Carlos III University of Madrid periodically to analyze the connectivity of its users.

The first step in developing the system was to study some network analysis tool to understand its operation and to implement a program according to their characteristics. The tool chosen for the study was the Fing application.

After the study, we proceeded to implement the code. In the first implementation of the requests on sequence, the time between each scan was not correct to carry on a significant following of connectivity. In the second implementation of the requests on parallel we obtained an adjustable time between scans, depending on the number of requests to be executed in each burst. With this mechanism we get to perform scans every 10 minutes, bringing a significant following of connectivity.

Having the system deployed, it was left scanning for an extended period of time to realize a study about the network. For this, we did an analysis of the results using graphs of various aspects of users connectivity, by accessing information stored in the database.

Finally, we can say that we have achieved all the objectives in this Bachelor Thesis, complying with the requirements set and it can be used for efficient network management.

7.2. Future works

Here some further improvements of the system implemented or proposed changes are listed:

- **Improvement Program:** Since the system's effectiveness depends on the interval of time in which each scan is done, you could try to monitor the network every 5 min or within the same scan only track users who are connected.

- **Monitoring in eduroam:** It would be interesting to realize a monitoring on the eduroam network, because currently the program does not work on that network. The causes are being investigated with the staff of IT services.

- **Extended period of time:** The initial idea of Bachelor Thesis is to continue with the analysis of the network for a quarter at least, in order to obtain more conclusive data.

- **Implementing Web:** Deploying a Web application where you can make inquiries in real time.

- **Assistance:** Keeping the monitoring for an extended period of time, could perform analysis on assistance by integrating schedules.

- **Location:** Scanning the network in different subnets and knowing the location and range of coverage of each, heat maps could be done with the movement of users within the network.

- **Detailed analysis:** Conducting more detailed analysis is future work of another Bachelor Thesis.

CAPÍTULO VII

ANEXOS

VIII. ANEXOS

En este capítulo se precisan todos los aspectos referentes a la gestión del proyecto, detallando la planificación del trabajo, los medios técnicos empleados para el desarrollo del TFG y el análisis económico del mismo.

8.1. Planificación

En la siguiente tabla se presenta el resumen de las tareas más relevantes a realizar, acompañado de su duración, junto con sus fechas de inicio y finalización.

Tarea	Inicio	Fin	Duración
Trabajo Fin de Grado	**20/09/14**	**24/02/15**	**158**
Documentación y estado del arte	**20/09/14**	**09/10/14**	**20**
Estudio redes inalámbricas	20/09/14	03/09/14	14
Estudio *Fing*	04/10/14	09/10/14	6
Diseño I	**10/10/14**	**21/11/14**	**43**
Desarrollo código	10/10/14	29/10/14	20
Instalación MySQL	30/10/14	30/11/14	1
Integración MySQL	31/10/14	10/11/14	11
Pruebas monitorización	11/11/14	21/11/14	11
Implementación consultas	**22/11/14**	**11/12/14**	**20**
Monitorización en serie	**12/12/14**	**11/01/15**	**31**
Diseño II	**09/01/14**	**22/01/15**	**14**
Desarrollo código	09/01/15	18/01/15	10
Pruebas monitorización	19/01/15	22/01/15	4

Monitorización en paralelo	**23/01/15**	**19/02/15**	**28**
Memoria	**25/01/15**	**24/02/15**	**31**
Organización y estructura	25/01/15	31/01/15	7
Redacción	01/02/15	24/0215	24

Tabla 5. Datos diagrama de Gantt

Con estos datos se ha realizado el diagrama de Gantt del proyecto (Figura 38):

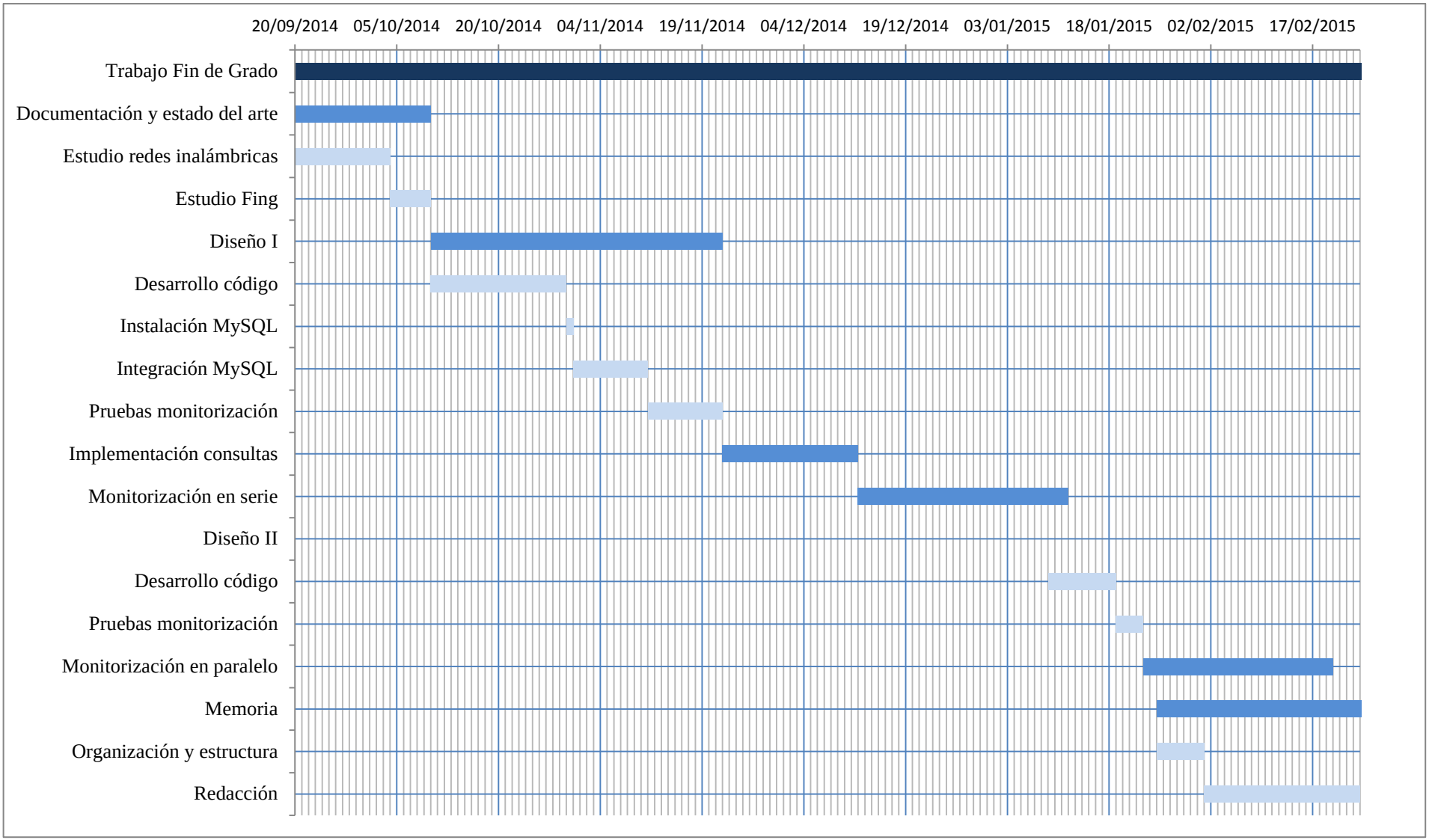


Figura 38. Diagrama de Gantt

8.2. Medios técnicos empleados

8.2.1. Hardware

- PC del laboratorio 4.1.F04 del Departamento de Ingeniería Telemática.
  - Nombre: Calamar
  - Kernel: 2.6.32-5-amd64
  - Procesador: Intel Core Quad (2.66 GHz)
  - RAM: 4 GB
  - Wireless

- Ordenador de sobremesa
  - Procesador: Intel Core i7 -2600k CPU @ 3.40 GHz
  - RAM: 16 GB

- Smartphone
  - Motorola Moto G
  - Procesador: Qualcomm Snapdragon 400 (1.2 GHz)
  - RAM: 1 GB

8.2.2. Software

- Sistemas Operativos:
  - GNU/Linux
  - Windows 7 Ultimate
  - Android 4.4.4

- Herramientas
  - Gedit
  - Wireshark
  - MySQL

- Suites ofimáticas
  - Microsoft® Office™ 2010 Professional

- Herramientas Web:
  - Dropbox
  - Highcharts

8.3. Marco regulador

En cuanto a restricciones legales, la Universidad Carlos III de Madrid permite el uso del acceso a internet mediante *WiFi-UC3M* exclusivamente para actividades docentes y de investigación, de acuerdo con los objetivos, funciones o responsabilidades asignadas a sus estudiantes, profesores y personal.

En el acuerdo sobre condiciones de uso para la conexión a *WiFi-UC3M* se comentan los siguientes aspectos:

"*Está expresamente prohibida la suplantación de direcciones de red, así como la utilización de identidades falsas. También está prohibida la difusión intencionada de contenidos inapropiados.*

El uso impropio de este recurso puede suponer la suspensión del servicio, sin perjuicio de las actuaciones disciplinarias y legales que pudieran derivarse. La Universidad Carlos III de Madrid se reserva el derecho de iniciar acciones oportunas en aquellos casos que, si bien no están directamente previstos en el presente Acuerdo, sí pueden estar contemplados en el Código Penal, o en cualquier otra normativa que resulte de aplicación. En este sentido debe tenerse en cuenta, entre otros, los artículos sobre daños físicos y a los programas: artículos 263 a 267 del Código Penal; sobre la propiedad intelectual y sobre la normativa relativa a la confidencialidad de la información."

Cabe destacar que en este Trabajo Fin de Grado no se realiza un uso que pueda calificarse contrario a las normas de uso de *WiFi-UC3M*, simplemente muestra la facilidad con la que se puede obtener información sobre el comportamiento de los usuarios de una red sin la necesidad de pedir autorización a los mismos. Por este motivo no se aplican más restricciones legales.

8.4. Análisis económico

- **Autor:** Mario Rodríguez Blanco
- **Departamento de Ingeniería Telemática**
- **Descripción del Proyecto**
  - **Título:** Análisis de la conectividad de usuarios en una red de campus 802.11
  - **Duración:** 5.6 meses
  - **Tasa de costes indirectos:** 20%
- **Presupuesto total del Proyecto:** ver tabla 4
- **Subcontratación de tareas:** No se especifica
- **Otros costes indirectos:** No se especifica

Concepto	Cantidad (€)	Coste (€)	% Proyecto	Dedicación (meses)	Depreciación (meses)	Total (€)
Recursos materiales						
PC del laboratorio	1	550	100	5.6	60	51,33
Ordenador de sobremesa	1		100	5.6	60	93,33
Smartphone	1	175	100	5.6	60	16,33
Subtotal						**160,99**
Recursos de trabajo						
Graduado Ing. Telemática	1 (5.6 Ing./mes)	2.694,39	-	-	-	1.508,58
Ingenieros Senior	2 (0.5 Ing./mes)	4.289,54	-	-	-	2.144,77
Subtotal						**17.233,35**
Otros costes						
Conexión a Internet	1	30	-	5.6	-	168
Subtotal						**168**
Total						**17.562,34 €**

Tabla 6. Presupuesto

BIBLIOGRAFÍA

[1] M. S. Gast, Wireless Networks: “The Definitive Guide”, O'Reilly, 2002.

[2] Gowex: Informe WiFi 2013 [En línea]
https://es.scribd.com/doc/206648696/GOWEX-Informe-WiFi-2013

[3] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2014–2019 [En línea]
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html

[4] J. F. Kurose, K.W Ross, “Redes de Computadores. Un Enfoque Descendente Basado en Internet”, Pearson S.A, 2003.

[5] J. Pang, 802.11 User *Fing*erprinting, 2007

[6] iOS 8: MAC Spoofeada en mensajes WiFi Probe Request [En línea]
http://www.seguridadapple.com/2014/09/ios-8-mac-spoofeada-en-mensajes-wifi.html

[7] Estándares 802 [En línea] http://www.ieee802.org/

[8] Servicio de red inalámbrica (WiFi) en la UC3M [En línea]
https://asyc.uc3m.es/index.php?Id=48

[9] Configuración *eduroam* [En línea] https://asyc.uc3m.es/index.php?Id=68

[10] RFC 826 ARP [En línea] http://www.ietf.org/rfc/rfc0826.txt

[11] Características *Fing* [En línea] http://www.overlooksoft.com/

[12] *Fing* en Android [En línea]
https://play.google.com/store/apps/details?id=com.overlook.android.Fing&hl=es

[13] *Fing* en iOS [En línea]
https://itunes.apple.com/es/app/Fing-networkscanner/id430921107?mt=8

[14] RFC 1034 DNS [En línea] https://www.ietf.org/rfc/rfc1034.txt

[15] RFC 1035 DNS [En línea] https://www.ietf.org/rfc/rfc1035.txt

[16] Carlos Jesús Bernardos, Manuel Urueña, Librería *librawnet*

[17] *Wpa_supplicant* [En línea] http://w1.fi/wpa_supplicant/

[18] MySQL [En línea] http://www.mysql.com/

[19] Marcas dispositivos [En línea] http://standards-oui.ieee.org/oui.txt

[20] Highcharts [En línea] http://www.highcharts.com/